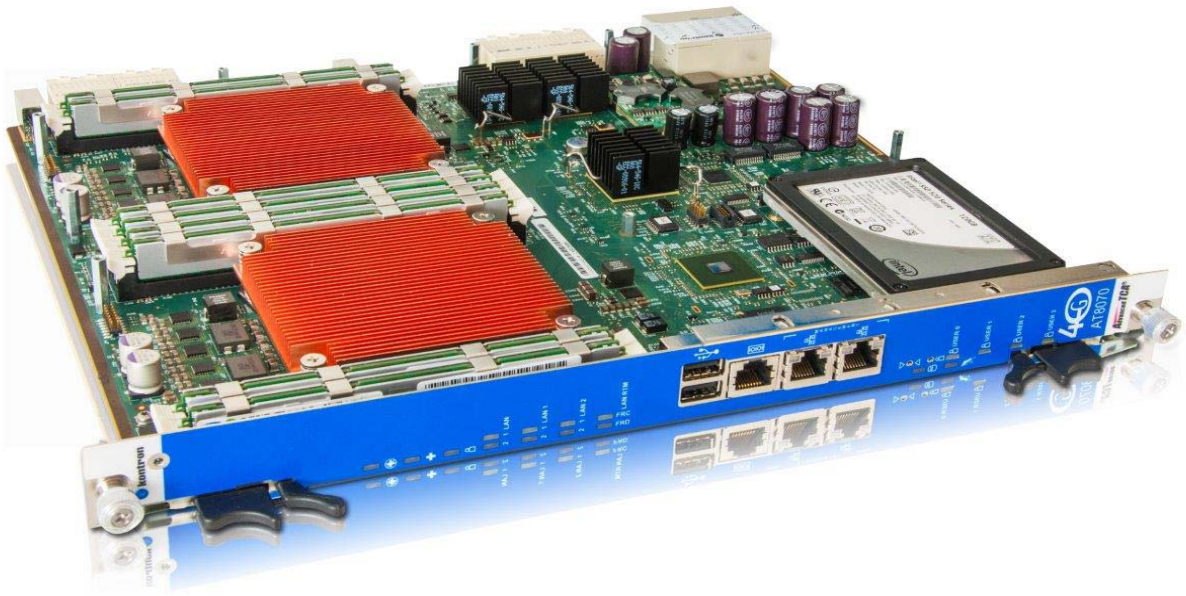
# »Kontron User's Guide«



## AT8070

Document Revision 1.0
November 2013

# Revision History

| Rev. Index | Brief Description of Changes | Date of Issue |
|---|---|---|
| 1.0 | First Release | November 2013 |
| | | |
| | | |
| | | |

# Customer Service


**Contact Information:**

**Kontron America**
14118 Stowe Dr
Poway, CA 92064-7147
Phone: (800) 480-0044
(US Only)
Fax: (858) 677-0898
support@us.kontron.com

**Kontron Canada, Inc.**
4555 Ambroise-Lafortune
Boisbriand, Québec, Canada
J7H 0A4
Tel: (450) 979-5320
(800) 354-4223
Fax: (450) 437-8053
support@ca.kontron.com

**Kontron Europe GmbH**
Sudetenstraße 7
87600 Kaufbeuren
Germany
+49 (0) 8341 803 333

+49 (0) 8341 803 40330
support@kontron.com

Visit our site at: www.kontron.com



© 2013 Kontron, an International Corporation. All rights reserved.

The information in this user's guide is provided for reference only. Kontron does not assume any liability arising out of the application or use of the information or products described herein. This user's guide may contain or reference information and products protected by copyrights or patents and does not convey any license under the patent rights of Kontron, nor the rights of others.

Kontron is a registered trademark of Kontron. All trademarks, registered trademarks, and trade names used in this user's guide are the property of their respective owners. All rights reserved. This user's guide contains information proprietary to Kontron. Customers may reprint and use this user's guide in other publications. Customers may alter this user's guide and publish it only after they remove the Kontron name, cover, and logo.

Kontron reserves the right to make changes without notice in product or component design as warranted by evolution in user needs or progress in engineering or manufacturing technology. Changes that affect the operation of the unit will be documented in the next revision of this user's guide.

# Table of Contents

*Safety Instructions* ..... *viii*

Before You Begin ..... viii

Preventing Electrostatic Discharge ..... ix

*Preface* ..... *x*

How to Use This Guide ..... x

Customer Comments ..... xi

Advisory Conventions ..... xi

Unpacking ..... xii

Powering Up the System ..... xii

Adapter Cables ..... xii

Storing Boards ..... xii

Regulatory Compliance Statements ..... xiii

Limited Warranty ..... xiv

*1. Product Description* ..... *2*

1.1 Product Overview ..... 2

1.2 What's Included ..... 2

1.3 Board Specifications ..... 3

1.4 Compliance ..... 5

1.5 Hot-Plug Capability ..... 5

1.6 Interfacing with the Environment ..... 5

1.6.1 RTM (rear transition module) ..... 5

*2. Board Features* ..... *8*

2.1 Block Diagram ..... 8

2.2 System Core ..... 9

2.2.1 Processors (SandyBridge-EP Series) ..... 9

2.2.2 Intel® C604 Chipset ..... 9

2.3 USB 2.0 Interfaces ..... 9

2.3.1 USB Flash Module ..... 10

2.4 Serial Attached SCSI ..... 10

2.5 Redundant BIOS Flash ..... 10

**2.6 Ethernet Interfaces . . . . . 10**
2.6.1 Fabric Interface . . . . . 10
2.6.2 Base Interface . . . . . 11
2.6.3 SFP ports on RTM. . . . . 11
2.6.4 RJ45 Management Ports . . . . . 12
**2.7 Serial Interfaces . . . . . 12**
**2.8 FPGA . . . . . 13**
**2.9 Redundant IPMC Firmware & BootBlock . . . . . 14**
**2.10 LEDs and push button Description . . . . . 14**
2.10.1 Hot Swap LED (LED0) . . . . . 14
2.10.2 Out Of Service (LED1) . . . . . 14
2.10.3 Healthy LED (LED2). . . . . 15
2.10.4 User LED . . . . . 15
2.10.5 Push button description. . . . . 15
***3. Installing the Board. . . . . 18***
**3.1 Setting Jumpers . . . . . 18**
3.1.1 Jumper Description . . . . . 18
**3.2 Processor . . . . . 18**
**3.3 Memory . . . . . 18**
3.3.1 Memory List and Characteristics . . . . . 19
3.3.2 Installing Memory . . . . . 21
**3.4 Onboard Connectors and Headers . . . . . 22**
**3.5 Board Hot Swap and Installation . . . . . 23**
3.5.1 Installing the Board in the Chassis. . . . . 24
3.5.2 Removing the Board . . . . . 24
3.5.3 Installing the RTM. . . . . 24
3.5.4 Removing the RTM . . . . . 24
***4. Management . . . . . 27***
**4.1 Hardware Management Overview . . . . . 27**
**4.2 Configuring LAN interface. . . . . 27**

**4.3 Web Management Interface . . . . . 27**
4.3.1 Connecting to the Web Management Interface . . . . . 27
4.3.2 System . . . . . 28
4.3.3 Sensor . . . . . 28
4.3.4 Event Log . . . . . 28
4.3.5 Control . . . . . 28
4.3.6 Maintenance . . . . . 29
4.3.7 Logout . . . . . 30
**4.4 Hardware Management Functionality . . . . . 30**
**4.5 IPMC Specific Features . . . . . 30**
4.5.1 Sensors . . . . . 31
**4.6 IPMC . . . . . 32**
4.6.1 Supported Commands . . . . . 32
4.6.2 Sensor Data Records . . . . . 40
4.6.3 FRU Information . . . . . 57
***5. Software Setup . . . . . 63***
**5.1 AMI UEFI Setup Program . . . . . 63**
5.1.1 Accessing the UEFI Setup Utility . . . . . 63
5.1.2 Menu Bar . . . . . 64
5.1.3 Main Menu . . . . . 66
5.1.4 Advanced Menu . . . . . 67
5.1.5 Chipset . . . . . 89
5.1.6 Server Management . . . . . 98
5.1.7 Boot . . . . . 103
5.1.8 Security . . . . . 104
5.1.9 Save & Exit . . . . . 104
**5.2 Boot Utilities . . . . . 105**
5.2.1 Entering BIOS Setup Menu . . . . . 105
5.2.2 SAS Option ROM (RTM806X) . . . . . 105
**5.3 Console Redirection (VT100 Mode) . . . . . 105**
5.3.1 Requirements . . . . . 105
5.3.2 ANSI and VT100 Keystroke Mapping . . . . . 106
5.3.3 VT-UTF8 Keystroke Mapping . . . . . 106
***A. Memory & I/O Maps . . . . . A-1***
**A.1 Memory Mapping . . . . . A-1**
**A.2 Kontron I/O Mapping . . . . . A-2**
**A.3 PCI IDSEL and Device Numbers . . . . . A-2**

*B. Connector Pinouts ..... B-1*

B.1 Connectors and Headers Summary ..... B-1
B.2 USB Connectors (J10) ..... B-1
B.3 Management Console Port (J11) ..... B-1
B.4 eUSB Flash Drive (J14) ..... B-2
B.5 Fabric Interface (J22) ..... B-2
B.6 Base Interface & Fabric Interface (J23) ..... B-3
B.7 RTM Connector (J30) ..... B-4
B.8 RTM Connector (J31) ..... B-4
B.9 Power (P10) ..... B-5

*C. BIOS Setup Error Codes ..... C-1*

C.1 Memory Reference Code ..... C-1
C.2 SEC Status Codes ..... C-2
C.3 PEI Status Codes ..... C-2
C.4 DXE Status Codes ..... C-4
C.5 ACPI/ASL Status Codes ..... C-6

*D. Software Update ..... D-1*

*E. Getting Help ..... E-1*

E.1 Returning Defective Merchandise ..... E-1
E.2 When Returning a Unit ..... E-2

*F. Glossary ..... F-1*

# List of Figures

Figure 2-1: Block Diagram . . . . . 8
Figure 2-2: Faceplate LEDs . . . . . 16
Figure 3-1: Jumper Description . . . . . 18
Figure 3-2: Onboard Connectors and Headers Locations . . . . . 23
Figure 4-1: E-Keying possibilities. . . . . 59

# List of Tables

Table 1-1 Board Specifications . . . 3
Table 2-1 SFP LED Significations . . . 12
Table 2-2 Serial Interface connector Pinout . . . 13
Table 2-3 Faceplate LEDs . . . 14
Table 3-1 Approved Memory List . . . 19
Table 3-2 Onboard Connectors and Headers . . . 22
Table 4-1 Privilege Level Description . . . 29
Table 4-2 IPM Device Supported Commands for IPMC . . . 32
Table 4-3 Watchdog Timer Supported Commands for IPMC . . . 32
Table 4-4 Device Messaging Supported Commands for IPMC . . . 32
Table 4-5 Chassis Device Supported Commands for IPMC . . . 34
Table 4-6 Event Supported Commands for IPMC . . . 34
Table 4-7 PEF and Alerting Supported Commands for IPMC . . . 35
Table 4-8 Sensor Device Supported Commands for IPMC . . . 35
Table 4-9 FRU Device Supported Commands for IPMC . . . 36
Table 4-10 SDR Device Supported Commands for IPMC . . . 36
Table 4-11 SEL Device Supported Commands for IPMC . . . 36
Table 4-12 LAN Device Supported Commands for IPMC . . . 37
Table 4-13 Serial/Modem Device Supported Commands for IPMC . . . 37
Table 4-14 SOL Commands . . . 38
Table 4-15 PICMG 3.0 Commands for IPMC . . . 38
Table 4-16 HPM Commands . . . 39
Table 4-17 IPMC Sensors . . . 40
Table 4-18 IPMC Health Indicator Sensor Aggregation Table . . . 56
Table 4-19 Board Information Area . . . 57
Table 4-20 Product Information Area . . . 58
Table 4-21 E-Keying capabilities of the board . . . 60
Table 4-22 Carrier AMC.0 . . . 61

# Safety Instructions

## Before You Begin

Before handling the board, read the instructions and safety guidelines on the following pages to prevent damage to the product and to ensure your own personal safety. Refer to the "Advisories" section in the Preface for advisory conventions used in this user's guide, including the distinction between Warnings, Cautions, Important Notes, and Notes.

- Always use caution when handling/operating the computer. Only qualified, experienced, authorized electronics service personnel should access the interior of the computer. The power supplies produce high voltages and energy hazards, which can cause bodily harm.
- Use extreme caution when installing or removing components. Refer to the installation instructions in this user's guide for precautions and procedures. If you have any questions, please contact Kontron Technical Support

**WARNING**

High voltages are present inside the chassis when the unit's power cord is plugged into an electrical outlet. Turn off system power, turn off the power supply, and then disconnect the power cord from its source before removing the chassis cover. Turning off the system power switch does not remove power to components.

# Preventing Electrostatic Discharge

Static electricity can harm system boards. Perform service at an ESD workstation and follow proper ESD procedure to reduce the risk of damage to components. Kontron strongly encourages you to follow proper ESD procedure, which can include wrist straps and smocks, when servicing equipment.

Take the following steps to prevent damage from electrostatic discharge (ESD):

- When unpacking a static-sensitive component from its shipping carton, do not remove the component's antistatic packing material until you are ready to install the component in a computer. Just before unwrapping the antistatic packaging, be sure you are at an ESD workstation or grounded. This will discharge any static electricity that may have built up in your body.
- When transporting a sensitive component, first place it in an antistatic container or packaging.
- Handle all sensitive components at an ESD workstation. If possible, use antistatic floor pads and workbench pads.
- Handle components and boards with care. Don't touch the components or contacts on a board. Hold a board by its edges or by its metal mounting bracket.
- Do not handle or store system boards near strong electrostatic, electromagnetic, magnetic, or radioactive fields.
- When you want to remove the protective foil (if present), make sure you are properly grounded and that you touch a metalic part of the board.

**CAUTION**

Removing the protective foil from the top and bottom cover might create static.
When you remove those protections, make sure you follow the proper ESD procedure.

# Preface

## How to Use This Guide

This user's guide is designed to be used as step-by-step instructions for installation, and as a reference for operation, troubleshooting, and upgrades.

For the circuits, descriptions and tables indicated, Kontron assumes no responsibility as far as patents or other rights of third parties are concerned.

The following is a summary of chapter contents:

- Chapter 1, Product Description
- Chapter 2, Board Features
- Chapter 3, Installing the board
- Chapter 4, Hardware Management
- Chapter 5, Software Setup
- Chapter 6, Thermal Considerations
- Appendix A, Memory & I/O Maps
- Appendix B, Connector Pinout
- Appendix C, BIOS Setup Error Codes
- Appendix D, Software Update
- Appendix E, Getting Help
- Appendix F, Glossary

# Customer Comments

If you have any difficulties using this user's guide, discover an error, or just want to provide some feedback, please send a message to: support@ca.kontron.com. Detail any errors you find. We will correct the errors or problems as soon as possible and post the revised user's guide on our Web site. Thank you.

# Advisory Conventions

Seven types of advisories are used throughout the user guides to provide helpful information or to alert you to the potential for hardware damage or personal injury. They are Note, Signal Paths, Jumpers Settings, BIOS Settings, Software Usage, Cautions, and Warnings. The following is an example of each type of advisory. Use caution when servicing electrical components.

**Note:**
Indicate information that is important for you to know.

**Signal Path:**
Indicate the places where you can find the signal on the board.

**Jumper Settings:**
Indicate the jumpers that are related to this section.

**BIOS Settings:**
Indicate where you can set this option in the BIOS.

**Software Usage:**
Indicates how you can access this feature through software.

**CAUTION**
Indicate potential damage to hardware and tells you how to avoid the problem.

**WARNING**
Indicates potential for bodily harm and tells you how to avoid the problem.

**ESD Sensitive Device:**
This symbol and title inform that electronic boards and their components are sensitive to static electricity. Therefore, care must be taken during all handling operations and inspections of this product, in order to ensure product integrity at all times.
Please read also the section "Special Handling and Unpacking Instructions".

**CE Conformity:**
This symbol indicates that the product described in this manual is in compliance with all applied CE standards. Please refer also to the section "Regulatory Compliance Statements" in this manual.

Disclaimer: We have tried to identify all situations that may pose a warning or a caution condition in this user's guide. However, Kontron does not claim to have covered all situations that might require the use of a Caution or a Warning.

# Unpacking

Follow these recommendations while unpacking:

- Remove all items from the box. If any items listed on the purchase order are missing, notify Kontron customer service immediately.
- Inspect the product for damage. If there is damage, notify Kontron customer service immediately.
- Save the box and packing material for possible future shipment.

# Powering Up the System

Before any installation or setup, ensure that the board is unplugged from power sources or subsystems.

If you encounter a problem, verify the following items:

- Make sure that all connectors are properly connected.
- Verify your boot devices.
- If the system does not start properly, try booting without any other I/O peripherals attached.

Make sure your system provides the minimum DC voltages required at the board's slot, especially if DC power is carried by cables.

If you are still not able to get your board running, contact our Technical Support for assistance.

# Adapter Cables

Because adapter cables come from various manufacturers, pinouts can differ. All cables are available from Kontron Sales Department.

# Storing Boards

Electronic boards are sensitive devices. Do not handle or store device near strong electrostatic, electromagnetic, magnetic or radioactive fields.

# Regulatory Compliance Statements

## *FCC Compliance Statement for Class B Devices*

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generated, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experience radio/TV technician for help.

**WARNING**

This is a Class B product. If not installed in a properly shielded enclosure and used in accordance with this User's Guide, this product may cause radio interference in which case users may need to take additional measures at their own expense.

## *Safety Certification*

All Kontron equipment meets or exceeds safety requirements based on the IEC/EN/UL/CSA 60950-1 family of standards entitled, "Safety of information technology equipment." All components are chosen to reduce fire hazards and provide insulation and protection where necessary. Testing and reports when required are performed under the international IECEE CB Scheme. Please consult the "Kontron Safety Conformity Policy Guide" for more information. For Canada and USA input voltage must not exceed -60Vdc for safety compliance.

## *CE Certification*

The product(s) described in this user's guide complies with all applicable European Union (CE) directives if it has a CE marking. For computer systems to remain CE compliant, only CE-compliant parts may be used. Maintaining CE compliance also requires proper cable and cabling techniques. Although Kontron offers accessories, the customer must ensure that these products are installed with proper shielding to maintain CE compliance. Kontron does not offer engineering services for designing cabling systems. In addition, Kontron will not retest or recertify systems or components that have been reconfigured by customers.

# Limited Warranty

Kontron grants the original purchaser of Kontron's products a TWO YEAR LIMITED HARDWARE WARRANTY as described in the following. However, no other warranties that may be granted or implied by anyone on behalf of Kontron are valid unless the consumer has the express written consent of Kontron.

Kontron warrants their own products, excluding software, to be free from manufacturing and material defects for a period of 24 consecutive months from the date of purchase. This warranty is not transferable nor extendible to cover any other users or long- term storage of the product. It does not cover products which have been modified, altered or repaired by any other party than Kontron or their authorized agents. Furthermore, any product which has been, or is suspected of being damaged as a result of negligence, improper use, incorrect handling, servicing or maintenance, or which has been damaged as a result of excessive current/voltage or temperature, or which has had its serial number(s), any other markings or parts thereof altered, defaced or removed will also be excluded from this warranty.

If the customer's eligibility for warranty has not been voided, in the event of any claim, he may return the product at the earliest possible convenience to the original place of purchase, together with a copy of the original document of purchase, a full description of the application the product is used on and a description of the defect. Pack the product in such a way as to ensure safe transportation (see our safety instructions).

Kontron provides for repair or replacement of any part, assembly or sub-assembly at their own discretion, or to refund the original cost of purchase, if appropriate. In the event of repair, refunding or replacement of any part, the ownership of the removed or replaced parts reverts to Kontron, and the remaining part of the original guarantee, or any new guarantee to cover the repaired or replaced items, will be transferred to cover the new or repaired items. Any extensions to the original guarantee are considered gestures of goodwill, and will be defined in the "Repair Report" issued by Kontron with the repaired or replaced item.

Kontron will not accept liability for any further claims resulting directly or indirectly from any warranty claim, other than the above specified repair, replacement or refunding. In particular, all claims for damage to any system or process in which the product was employed, or any loss incurred as a result of the product not functioning at any given time, are excluded. The extent of Kontron liability to the customer shall not exceed the original purchase price of the item for which the claim exists.

Kontron issues no warranty or representation, either explicit or implicit, with respect to its products reliability, fitness, quality, marketability or ability to fulfil any particular application or purpose. As a result, the products are sold "as is," and the responsibility to ensure their suitability for any given task remains that of the purchaser. In no event will Kontron be liable for direct, indirect or consequential damages resulting from the use of our hardware or software products, or documentation, even if Kontron were advised of the possibility of such claims prior to the purchase of the product or during any period since the date of its purchase.

Please remember that no Kontron employee, dealer or agent is authorized to make any modification or addition to the above specified terms, either verbally or in any other form, written or electronically transmitted, without the company's consent.

*Chapter 1*

# Product Description


1.1 Product Overview ..... 2
1.2 What's Included ..... 2
1.3 Board Specifications ..... 3
1.4 Compliance ..... 6
1.5 Hot-Plug Capability..... 6
1.6 Interfacing with the Environment ..... 6

# 1. Product Description

## 1.1 Product Overview

The AT8070 is a 40G ATCA Dual Intel Xeon Processor blade. It brings to our ATCA board family the Dual-Dual Star Fabric Interface capability for the first time.

The core of the AT8070 is featuring two Intel® Xeon® Processor E5-2600 Product Family “Sandy Bridge” and the Intel® C604 Chipset (Intel® BD82C604 PCH) “Patsburg”. Each processor is connected to four channels of DDR3 memory for up to 128GB. Both processors are connected together via 2 channels of the Intel® QPI link.

The Dual-Dual Star Fabric Interface is provided by Two Mellanox ConnectX®-3 EN at 40Gpbs/10Gpbs/1Gbps.

The Base Interface is provided by Intel® 82576EB Gigabit Ethernet Controller at 1Gbps.

Other Ethernet connections are provided by the Intel® Ethernet Controller I350-AM4: two RJ45 face plate connections and two RTM SFP connections at 1Gbps.

Other accessible interfaces are:

- Onboard drive 2.5" SAS/SATA HDD/SSD
- 2 USB ports on the front panel
- 1 eUSB onboard
- 1 serial console on the front panel

The board is compatible with the Rear Transition Module RTM8063-CC with 2 hot swap 2.5’’ SAS/SATA hard drives. The I/O available on the RTM connectors are: x8 PCIe Gen2, 3 SAS interfaces, 2 USB, 2 SFP ports, Serial port.

The AT8070 operates in two power level modes, a regular power mode up to 225W for NEBS-like operation and a High Power mode up to 350W for higher-class chassis applications.

## 1.2 What’s Included

This board is shipped with the following items:

- One AT8070 board
- One RJ45-DB9 serial adaptor (1015-9404)

If any item is missing or damaged, contact the supplier.

# 1.3 Board Specifications

Table 1-1: Board Specifications

| Features | Description |
|---|---|
| Processors | Dual Intel® Xeon® Processor E5-2600 Family; Passive heatsink<br>• 8cores 1.8GHz 70W<br>• 8cores 2.0GHz 95W<br>• 6cores 2.3GHz 95W |
| Chipset | • Intel® C604 Chipset (Intel® BD82C604 PCH) "Patsburg" |
| Bus Interface | • Dual QPI 8GT/s between both CPUs<br>• DMI Gen2 5GT/s from CPU to Chipset |
| Expansion Slot | • PCIe x8 Gen2 connection to RTM |
| System Memory | • Support of DDR3 1066 to 1600MHz with ECC<br>• Standard voltage(1.5V) and low-voltage(1.35V) modules are supported<br>• 4 memory channnels per CPU with a single DIMM location per channel<br>• Up to 16GB memory modules per socket for a total of 128GB |
| Flash Memory | • One connector for an optional eUSB (embedded USB) flash drive module. |
| Storage | • One onboard 2.5" SAS/SATA HDD Connector. SATA GEN1 (1.5Gb/s), GEN2 (3Gb/s), GEN3 (6Gb/s) and SAS 3Gb/s compatible.<br>• Three SATA GEN1 (1.5Gb/s), GEN2 (3Gb/s), GEN3 (6Gb/s) and SAS 3Gb/s storage interfaces on the RTM. |
| I/O | Faceplate connectors:<br>• Dual RJ45 1Gb/s connector<br>• Dual USB<br>• RJ45 Serial Port<br>• Internal/Backplane<br>• TPM (optional)<br>• Fabric Interface (Dual-Dual Star): Mellanox ConnectX-3 40Gb/s, 10Gb/s or 1Gb/s Ethernet Controller<br>• Base Interface: Intel i82576 1Gb/s<br>RTM Connectors (optional add-on):<br>• Video debug header (available upon request)<br>• Dual SFP 1Gb/s connector |
| Board Specifications | • PICMG3.0 R3.0(AdvancedTCA Base Specification)<br>• PICMG3.1 R1.0 (Ethernet/Fiber Channel over AdvancedTCA)<br>• ACPI rev 2.0<br>• HPM.1<br>• IPMI 2.0 |

| Features | Description |
|---|---|
| BIOS Features | • AMI UEFI with Compatibility Support Module for legacy option ROMs and Operating System support<br>• Save BIOS Configuration to SPI.<br>• Boot from Ethernet PXE (Base and management Lan)<br>• Boot from SAS/SATA; and boot from USB 2.0 (Floppy, CD-ROM, Hard Disk)<br>• Diskless, Keyboard less, and battery less operation extensions<br>• System, video and LAN BIOS shadowing<br>• Robust BIOS flash Update with rollover capability (HPM.1)<br>• Field updateable BIOS<br>• Advanced Configuration and Power Interface (ACPI 2.0, 3.0 & 4.0)<br>• Console redirection to serial port (VT100)with CMOS setup access, and SOL (Serial over LAN)<br>• Event (correctable/uncorrectable ECC,PCIe, POST errors); log support to IPMC |
| IPMI Features | • Management Controller compliant IPMI v2.0.<br>• Remote control capability (power on-off /clean shutdown/cold reset) via any IPMI channels including LAN.<br>• Full speed 115200 bps Serial Over LAN (+LAN access to BIOS menu setup) and IPMI Over LAN (IPMI v2.0) always available.<br>• Serial data caching and replay to ease software application troubleshooting and post mortem analysis.<br>• Bios Post Code errors are sent to the chassis manager's for System Event Logging.<br>• Configurable automatic “clean ACPI shutdown” policy on disk storage deactivation.<br>• Standard PCIe Hot Plug operation embedded with PICMG RTM activation.<br>• Robust IPMI firmware Update with rollover capability, without any payload impact (HPM.1).<br>• Override configuration for activation of the board/RTM without Shelf Manager Intervention. |
| Supervisory | • Supports a system management interface (KCS interrupt driven) via an IPMI V2.0 compliant controller.<br>• Standard IPMI Watchdog for all CPU running phases (BIOS execution / OS loading and running).<br>• IPMI Hardware system monitor (power/voltages), memory and all critical component's is monitored.<br>• Extensive sensor monitoring (around 100 IPMI sensors) and event generation based on thresholds and discrete readings. |
| OS Compatibility | • Validated with: Red Hat Enterprise 6.3 / CentOS 6.3. |
| Power Requirements | 1- NEBS power mode: = < 235W (25W RTM)<br>2- High power mode: = < 350W |
| Environmental Temperature* | Operating: 0-55°C/32-131°F with 40CFM airflow; for the 70W CPU configuration<br>Storage and Transit: -40 to +70°C/-40 to 158°F |
| Environmental Humidity* | Operating: 15% to 90% @55°C/131°F non-condensing<br>Storage and Transit: 5% to 95% @ 40°C/104°F non-condensing |
| Environmental Altitude* | Operating: 4,000 m / 13,123 ft<br>Storage and Transit: 15,000 m / 49,212 ft |
| Environmental Shock* | Operating: 3G each axis<br>Storage and Transit: 18G each axis |

| Features | Description |
|---|---|
| Environmental Vibration* | Operating: 5-200Hz. 0.2G, each axis<br>Storage and Transit: 5Hz to 20Hz @ 1 m2/s3 (0.01g2 /Hz) (flat)<br>20Hz to 200Hz @ -3dB/oct (slope down) |
| Reliability | • Whole board protected by active breaker<br>• USB voltage protected by active breaker |
| Safety / EMC | Meet or exceed:<br>• Safety: UL 60950-1; CSA C22.2 No 60950-1-03; EN 60950-1:2001; IEC60950-1<br>• EMI/EMC: FCC 47 CFR Part 15, Class B; CE Mark to EN55022/EN55024/EN300386 |
| Warranty | Two years limited warranty |

* Designed to meet or exceed

# 1.4 Compliance

This product conforms to the following specifications:

- PICMG3.0 R3.0(AdvancedTCA Base Specification)
- PICMG3.1 R2.0 Option 1, 9-K and 9-KR (Ethernet over Fabric Interface)
- ACPI rev 2.0
- HPM.1
- IPMI 2.0

# 1.5 Hot-Plug Capability

The AT8070 supports Full Hot Swap capability as per PICMG3.0 R3.0 for the board itself and the RTM module. It can be removed from or installed in the system while it is on (without powering-down the system). Please refer to the PICMG3.0 R3.0 specification for additional details about Hot Swap.

The AT8070 supports PCI-Express Hotplug on RTM. The IPMC uses the standard PCI Express Hotplug Controller on the CPU board allowing hot insertion and removal of a RTM module within the OS.

# 1.6 Interfacing with the Environment

## 1.6.1 RTM (Rear Transition Module)

The AT8070 supports different single slot (6HP) AdvancedTCA Rear Transition Modules: RTM806X. These modules provide additional connectivity for AT8070 CPU front blade. Please refer to the manual of the compatible RTM module for more details on implemented ports and devices.

### *1.6.1.1 Standard Compliance*

- PICMG3.0 R3.0 - Advanced Telecommunication Computing Architecture

### *1.6.1.2 I/O interconnects available to the RTM connector:*

- x8 PCIe Gen2
- 3 SAS Interfaces
- 2 USB Ports
- 2 SFP 1Gbps Ports

- 1 Serial Port.

#### 1.6.1.3 Serial Port Feature

- One serial port available on the RTM face plate through a RJ-45 connector.
- RS-232 signal levels at RTM face plate connector.
- Serial port speed capability is: 9.6kbits/s to 115.2kbits/s.

#### 1.6.1.4 Debug Video Feature

A header is present on the RTM to connect a debug video cable. This interface is suitable for low rate video, not for HD or intensive use. Video signals are VGA standard signals. Custom video cable available upon request - please contact Technical Support.

#### 1.6.1.5 Hot Swap

The RTM supports hot swapping by using a microswitch connected to the face plate's lower ejector handle. This switch indicates the coming hot swap action. The insertion of the RTM to a slot is always done over a non powered connector. During the extraction procedure, the management power is disabled only when the RTM806X is removed. This procedure meets the AdvancedTCA RTM behavior.

##### 1.6.1.5.1 Inserting the RTM into the slot

The presence of the RTM is indicated by one signal, The front blade's IPMC recognizes as an RTM insertion when the signal is low. After recognizing the RTM, the IPMC turns the blue LED ON and enables the management power to the RTM. Once the IPMB-L link is working, the IPMC accesses the MMC to retrieve FRU data. After knowing the type of RTM inserted, the IPMC negotiates with the shelf manager in order to activate the +12V payload power.

After RTM local voltages ramp up, the front board IPMC informs the shelf manager there is a functional RTM blade present.

##### 1.6.1.5.2 Removing the RTM from the slot

The RTM_EJECT signal goes HIGH by opening the RTM lower ejector handle. This indicates to the front blade IPMC that a hot swap action is going to take place. The IPMC then negotiates the removal with the System manager and if it is granted, it proceeds with the deactivation process.

The IPMC proceeds to the deactivation by disabling ekeying-governed links, then the IPMC then turns OFF the payload +12V power. When it is safe to remove the RTM blade from the slot, the IPMC turns the Blue / Hot Swap LED ON. Front Blade IPMC turns OFF the management power only when there is no RTM detected. (RTM806X removed from the slot)

*Chapter 2*

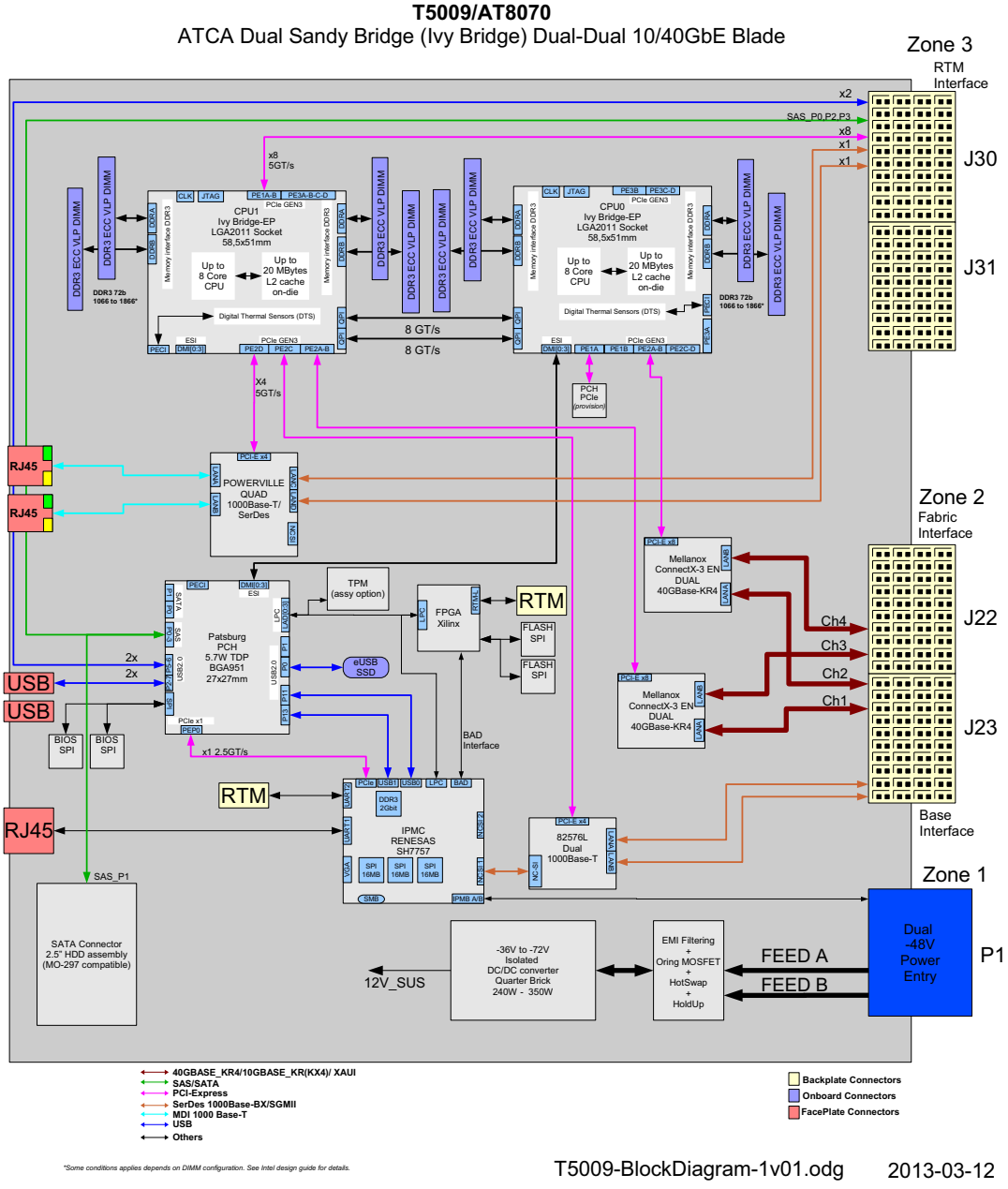
# Board Features


2.1 Block Diagram ..... 8
2.2 System Core ..... 9
2.3 USB 2.0 Interfaces..... 9
2.4 Serial Attached SCSI ..... 10
2.5 Redundant BIOS Flash ..... 10
2.6 Ethernet Interfaces..... 10
The supported speeds are : 10/100/1000Base-T. ..... 12
2.7 FPGA..... 13
2.8 Redundant IPMC Firmware & BootBlock..... 13
2.9 LEDs and push button Description..... 13

# 2. Board Features

## 2.1 Block Diagram

Figure 2-1:Block Diagram



# 2.2 System Core

## 2.2.1 Processors (SandyBridge-EP Series)

- Built on 32 nanometer process technology.
- Six/Eight cores processor in 2011-land FCLGA.
- 32KB L1/core
- 256KB L2 / core
- Up to 20MB L3: Up to 2.5MB per core.
- Streaming SIMD Extension 4.1 and 4.2
- Integrated 4-channel DDR3 controller, DDR3-1600 memory with ECC
- Intel QuickPath interconnect links, 8.0/7.2 GT/s in each direction
- Intel 64-Bit Architecture
- Enhanced Intel SpeedStep Technology
- Intel Virtualization Technology (VT)
- Intel Hyper-Threading Technology (HT)

## 2.2.2 Intel® C604 Chipset

- Direct Media Interface (DMI) x4 lanes for communicating with CPU0
- SATA Gen3 up to 6Gbps, SAS Gen2 up to 3Gbps, USB, PCIe

# 2.3 USB 2.0 Interfaces

The board embeds a USB controller in the PCH. This controller is compliant to USB 2.0. It provides two USB ports on the face plate, two on the RTM and two ports are reserved for the eUSB SSD. Those ports can be used for external storage and for booting.

USB supports Plug and Play and hot-swapping operations (OS level). These features allow USB devices to be automatically attached, configured and detached, without reboot or running setup.

**Signal Path:**
- 2 USB 2.0 on face plate (J10)
- 2 USB 2.0 on the RTM face plate
- 1 USB 2.0 onboard for the eUSB SSD (J14)

**BIOS Settings:**
Advanced -> USB Configuration
Chipset -> South Bridge -> USB Configuration

### 2.3.1 eUSB Flash Module

The AT8070 supports one Solid State Drive. It is a NAND flash disk module with a USB 2.0 interface. The module is socketed on a 2x5 header attached to the AT8070. It is available in many sizes and accessible only by removing the top cover. When connected, the eUSB SSD is automatically added to the 'bootable devices' list.

**Signal Path:**
USB Flash Module Connector is available on J14. See section 3.4 for more details.

**BIOS Settings:**
Advanced --> USB Configuration
Boot --> BBS

**Note:**
During the installation of an OS on a HDD, the USB Flash Module must be deactivated. If the USB Flash Module remains active, the Master Boot Record will be installed on it by default. This can not be avoided and will cause the OS to be unable to boot from the HDD.

## 2.4 Serial Attached SCSI

The PCH's SAS ports 0, 2, 3 are available through the RTM connector. The port 1 is accessible directly onboard.The supported mode are: SATA GEN1 (1.5Gb/s), GEN2 (3Gb/s), GEN3 (6Gb/s) and SAS 3Gb/s.

## 2.5 Redundant BIOS Flash

Two redundant 64MBits, SPI EEPROMs are connected to PCH for the BIOS. Only one EEPROM at a time is available for the PCH. If for some reason a BIOS update corrupts an EEPROM which prevents the CPU from completing the boot sequence, the IPMC will swap the active SPI EEPROM and force a reboot.

## 2.6 Ethernet Interfaces

### 2.6.1 Fabric Interface

The AT8070 features a Dual-Dual Star connection to the Fabric Interface.

The connections are provided by two Mellanox ConnectX-3. Each controller is connected to its own CPU and in order to provide a direct access for each CPU to the basic Dual Star ports (FI 1,2)

CPU0 - ConnectX-3_1 - Fabric Channel 2 and 4 - Linux eth0 and eth1

CPU1 - ConnectX-3_2 - Fabric Channel 1 and 3 - Linux eth2 and eth3

The fabric interface can be either 40GbE - 40GBASE-KR4; 10GbE - 10GBASE-KX4(XAUI); 1GbE - 1000BASE-KX. An E-Keying configuration is required to properly route the desired connection speed.

Refer to http://www.mellanox.comfor addictional details on the ConnectX-3.

**Signal Path:**
The four ports are available on the Fabric Interface as per PICMG 3.0 Revision 3.0 AdvancedTCA Base Specification.

## 2.6.2 Base Interface

An i82576EB dual port 1Gb Ethernet controller is connected to the Base Interface.

Boot from LAN capability (PXE) is supported on these ports. Enable the option from the BIOS Setup Program. For more details, please refer to Section 5.1, AMI UEFI Setup Program.

Features high performance with TCP/IP and UDP/IP checksum offloading for IPv4 and IPv6, packet filtering, and jumbo frames up to 16K.

See http://www.intel.com for additional details on the i82576EB.

**Signal Path:**
The two ports are available on the Base Interface.

## 2.6.3 SFP ports on RTM

Two 1GbE SFP ports are provided to the RTM by the i350 Ethernet Controller (Powerville) installed on the board. Boot from LAN capability (PXE) is supported on these ports. Enable the option from the BIOS Setup Program. Please refer to Section 5.1, AMI UEFI Setup Program.

**Signal Path:**
Two SFP ports are available on the RTM.

**BIOS Settings:**
Advanced --> Legacy Expansion ROM Configuration -> FP: GE OpROM, Port 1 and 2 (front panel)-> RTM:

**CAUTION LASER LIGHT!**

Do not look into the laser beam!
The SFP module is fitted with a class 1 or 1M laser. To avoid possible exposure to hazardous levels of invisible laser radiation, do not exceed maximum ratings.

Each SFP port has a bi-color green/amber LED with the following signification:

Table 2-1: SFP LED Significations

| LED | Signification |
|---|---|
| Green on | Link 1Gbit |
| Green blink | Activity 1Gbit |
| Amber on | Link 10/100Mbit |
| Amber blink | Activity 10/100Mbit |

## 2.6.4 RJ45 Management Ports

Two 1GbE RJ45 management ports are provided to the AT8070 face plate by the i350 Ethernet Controller (Powerville) installed on onboard. Boot from LAN capability (PXE) is supported on these ports. Enable the option from the BIOS Setup Program.

Please refer to Section 5.1, AMI UEFI Setup Program.

The supported speeds are : 10/100/1000Base-T.

**Signal Path:**
Two SFP ports are available on the RTM.

**BIOS Settings:**
Advanced -> Legacy Expansion ROM Configuration -> FP: GE OpROM, Port x

The AT8070 uses serial interfaces to manage the CPU, which is the only way to get visual information from the board when used without an RTM806X. Serial ports are provided on the faceplate and on the RTM faceplate for asynchronous serial communications. They are 16C550 high-speed UART compatible and support 16-byte FIFO buffers for transfer rates from 9,6Kbps to 115,2Kbps.

Table 2-2:Serial Interface connector Pinout

| Pin | Signal |
|---|---|
| 1 | RTS |
| 2 | DTR |
| 3 | TX# |
| 4 | GND |
| 5 | GND |
| 6 | RX# |
| 7 | DSR |
| 8 | CTS |

**Note:**
Standard product uses a RJ-45 8 pins connector. RI (ring indicator) and DCD (data carrier detect) signals are not available.
The pinout is a custom one, not the same as RS-232D TIA/EIA-561.

**Signal Path:**
COM1 is routed to an RJ45 jack on the faceplate or to the IPMC for SOL.
COM2 is routed to the RTM serial interface.

**BIOS Settings:**
Advanced -> Serial Port Console Redirection -> Console Redirection Settings (COM1 and COM2)

## 2.7 FPGA

The FPGA has many functions; One of them is to act in concert with the IPMC. The states of all the critical signals controlled by the IPMC are memorized in the FPGA and are preserved while the IPMC firmware is being updated.

The FPGA is a RAM-based chip that is preloaded from a separate flash memory at power-up. Two such flash memory devices are provided; one that can only be programmed in factory and the other one that can be updated in the field. The factory flash is selected by inserting jumper JP2 pins 3-4. Field updates require a power-cycle of the board. The IPMI LED2 will blink amber if the factory flash is being used, to signaling a fail-safe configuration.

The FPGA update complies to PICMG HPM.1 specification and is remotely updatable via any IPMC channel.

## 2.8 Redundant IPMC Firmware & BootBlock

The IPMC runs firmware loaded from SPI flash memory. The IPMC Boot Block saves the last two copies of the IPMC firmware image and manages bank states. It can also rollback to the previous firmware image in flash in case of errors following an update, etc.

## 2.9 LEDs and push button Description

The following table lists the LEDs on the faceplate.

Table 2-3:Faceplate LEDs

| LED Name | Color | Controlled by | Description |
|---|---|---|---|
| HDD activity | Green | Chipset/FPGA | Onboard & RTM HDD activity status |
| ATCA0 | Blue | IPMC | Blade Hot Swap status |
| ATCA1 | Amber/Red | IPMC | Blade OOS (out-of-service) |
| ATCA2 | Amber/Green | IPMC | Healthy status |
| ATCA3 | Amber/Green | IPMC/CPU | User-configurable |
| B.I. 1 | Amber/Green | FPGA | Base Interface Channel 1 Status |
| B.I. 2 | Amber/Green | FPGA | Base Interface Channel 2 Status |
| F.I. 1 | Amber/Green | FPGA | Fabric Interface Channel 1 Status |
| F.I. 2 | Amber/Green | FPGA | Fabric Interface Channel 2 Status |
| RTM 1 | Amber/Green | FPGA | Management LAN RTM Interface Channel 1 status |
| RTM 2 | Amber/Green | FPGA | Management LAN RTM Interface Channel 2 status |

### 2.9.1 Hot Swap LED (ATCA0)

The Blue / Hot Swap LED indicates the hot swap status of the unit. The LED is ON when it is safe to remove the unit from the slot. During normal operation, this LED is OFF.

Solid On (100 % on): FRU Inactive

Long Blink ( 90 % on): FRU Activation Request

Solid Off ( 0 % on): FRU Activation In Progress / FRU Active

Short Blink ( 10 % on): FRU Deactivation Request / FRU Deactivation In Progress

### 2.9.2 Out Of Service (ATCA1)

The AdvancedTCA LED1 is red or amber and indicates an Out-of-Service (OOS) condition. During normal operation, the OOS LED is OFF. This LED is ON when IPMC is in reset or starting up, and is user-configurable if needed, by a customer application.

### 2.9.3 Healthy LED (ATCA2)

The AdvancedTCA LED2 is green or amber and indicates a healthy condition. The healthy LED indicates if the blade is powered up and all voltages and temperatures are within specifications. During normal operation, this LED is ON (green). This LED is also ON (amber) when one of the RTM806X voltage or temperature sensors report a critical threshold reading.

Off: Payload power down

Green: Health Ok

Amber: Health Error (Critical)

Application Defined: May be controlled by application using PICMG API

## 2.9.4 User LEDs

### *2.9.4.1 ATCA User LED (LED3)*

The AdvancedTCA LED3 is green and/or amber. This LED is controlled by the IPMC and its state can be controlled using 'ipmitool picmg led' commands or other ATCA-compliant API.

### *2.9.4.2 Customer-configurable LEDs*

On the AT8070 we added 4 new user LEDs.

- User LED0 - Green/Amber
- User LED1 - Red/Amber
- User LED2 - Red/Amber
- User LED3 - Red/Amber

Please contact technical support for more informations.

## 2.9.5 Push button description

### *2.9.5.1 Reset button*

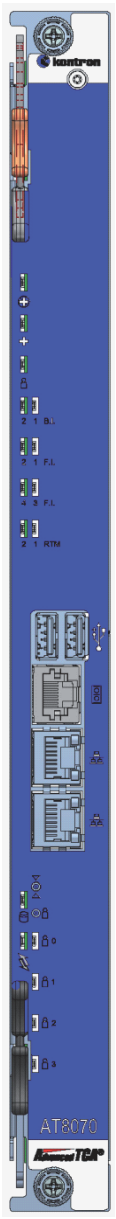
This switch will initiate a system cold reset

### *2.9.5.2 Debug/User button*

This button is user defined.

Please contact technical support for more informations.

Figure 2-2:Faceplate LEDs




**Hot Swap (Blue)**

Solid On (100 % on): FRU Inactive
Long Blink ( 90 % on): FRU Activation Request
Solid Off ( 0 % on): FRU Activation In Progress / FRU Active
Short Blink ( 10 % on): FRU Deactivation Request / FRU Deactivation In Progress

**Out of service (Red/Amber) [ default : Red ]**

Solid On : MMC in reset
Fast Blink (~50 % on) : MMC upgrade/rollback in progress
Application Defined : May be controlled by application using PICMG API

**Health Led (Amber/Green) [ default : Green ]**

Off : Payload power down
Green : Health Ok
Amber : Health Error (Critical)
Application Defined : May be controlled by application using PICMG API

**Hard Disk Activity Led (Green)**

Blink : Hard Disk Activity

**FI Led (Green/Amber)**

Green On : Link
Green Blink : Activity

**BI Led (Green/Amber)**

Green On : Link 1Gbit
Green Blink : Activity 1Gbit
Amber On : Link 10-100Mbit
Amber Blink : Activity 10-100Mbit

**SPM RTM Led (Green/Amber)**

Green On : Link 1Gbit
Green Blink : Activity 1Gbit
Amber On : Link 10-100Mbit
Amber Blink : Activity 10-100Mbit

**1GigE RJ45 Connector**

LED 1 Green Off : No link
LED 1 Green On : Link
LED 1 Green Blink : Activity
LED 2 Off : No link
LED 2 Amber : Link 10-100Mbit
LED 2 Green : Link 1Gbit

*Chapter 3*

# Installing the Board


3.1 Setting Jumpers ..... 18
3.2 Processor ..... 18
3.3 Memory ..... 18
3.4 Onboard Connectors and Headers ..... 21
3.5 Board Hot Swap and Installation ..... 22

# 3. Installing the Board

## 3.1 Setting Jumpers

### 3.1.1 Jumper Description

Figure 3-1:Jumper Description

| Name | Description | Jumper |
|---|---|---|
| WatchDogs Disable | WatchDogs Disable | JP1 (1-2) |
| Shelf Manager Override | Override if install | JP1 (3-4) |
| IPMI Override | Override (FPGA turn-on blade) | JP1 (5-6) |
| FRU Override | Override (Turn-on FRUs) | JP1 (7-8) |
| Spare | Reserved | JP2 (1-2) |
| FPGA PROM Selection | Factory PROM (Fail-Safe) | JP2 (3-4) |
| Clear BIOS Setup In Flash | Reserved | JP2 (5-6) |
| Reserved | Reserved | JP2 (7-8) |
| FRU PCIe Override | Override (drive FRUs clocks) | JP1 (9-10) |
| Reserved | Reserved | JP1 (11-12) |
| Reserved | Reserved | JP1 (13-14) |
| Reserved | Reserved | JP2 (9-10) |
| Reserved | Reserved | JP2 (11-12) |
| Onboard Video Enable | RTM Video Enabled | JP1 (13-14) |

**Note:**
More details about the jumper settings can be found on the Quick Reference Sheet.

## 3.2 Processor

This product can be shipped with the CPUs and a thermal solution installed. The thermal solution is custom-designed and critical for effective passive cooling. Cooling performance can greatly be affected if heat sink is not handled properly. Do not attempt any heat sink removal after installation.

## 3.3 Memory

The AT8070 has 4 memory channels connected to each CPU. There is one DIMM per memory channel for a total of 4 per CPU.

Memory should have the following characteristics:

- DDR3 1333 or 1600
- 1.35V or 1.5V

- x4 or x8 memory with up to 4 ranks per DIMM
- registered or unbuffered
- ECC
- VLP(very low-profile - 0.72 inch, 18.29mm) or ULP (ultra low-profile - 0.699inch, 17.75mm). The maximum DDR3 SDRAM size is 16GBytes per DIMM for a populated 128GBytes maximum.

Memory modules shall have a validated thermal solution (heatsink) and may necessitate a certain class of chassis. It is recommended that modules have thermal sensors for accurate temperature monitoring and to throttle the memory interface in case of overheating. Kontron recommends the use of validated memory with this product. Thermal issues or other problems may arise if you don't use recommended modules. At the time of publication of this user guide, the following memories memory list have been qualified and approved. As the memory market is volatile, this list is subject to change, please consult technical support for an up to date list.

### 3.3.1 Memory List and Characteristics

Table 3-1:Approved Memory List

| Manufacturer Part Number | Description | Company |
|---|---|---|
| M392B5273DH0-CK0 | 4GB VLP 1600 MHz RDIMM | Samsung |
| M392B1K70DM0-CK0 | 8GB VLP 1600 MHz RDIMM | Samsung |
| M392B5273CH0-YH9 | 4GB VLP 1333 MHz LV-RDIMM | Samsung |
| VL33B5263E-K9S | 4GB VLP 1333 MHz RDIMM | Virtium |
| M392B2G70BM0-YK0 | 16GB VLP 1600 MHz RDIMM | Samsung |
| SGU04G72H1BC2SA-BBRT | 4GB VLP 1333 MHz UDIMM | Swissbit |
| MT18JDF1G72PDZ-1G6 | 8GB VLP 1600 MHz RDIMM | Micron |
| MT36JDZS2G72PZ-1G9E1 | 16GB VLP 1866 MHz RDIMM | Micron |

**WARNING**

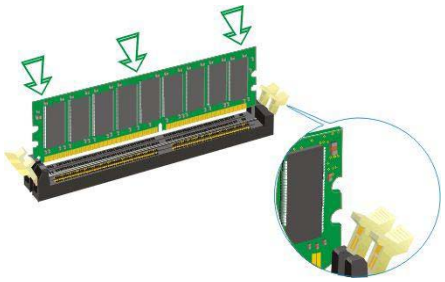
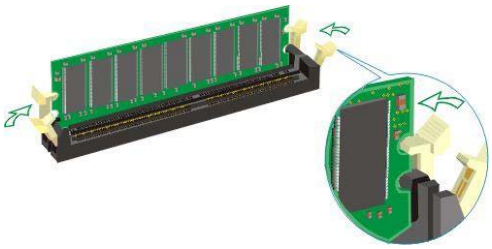
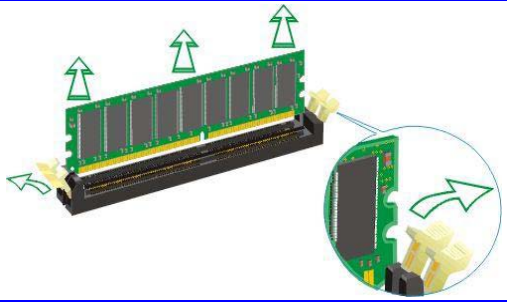
Because static electricity can cause damage to electronic devices, take the following precautions:

Keep the board in its anti-static package, until you are ready to install memory.

Wear a grounding wrist strap before removing the board from its package; this will discharge any static electricity that may have built up in your body.

Handle the board by the faceplate or its edges.

## 3.3.2 Installing Memory

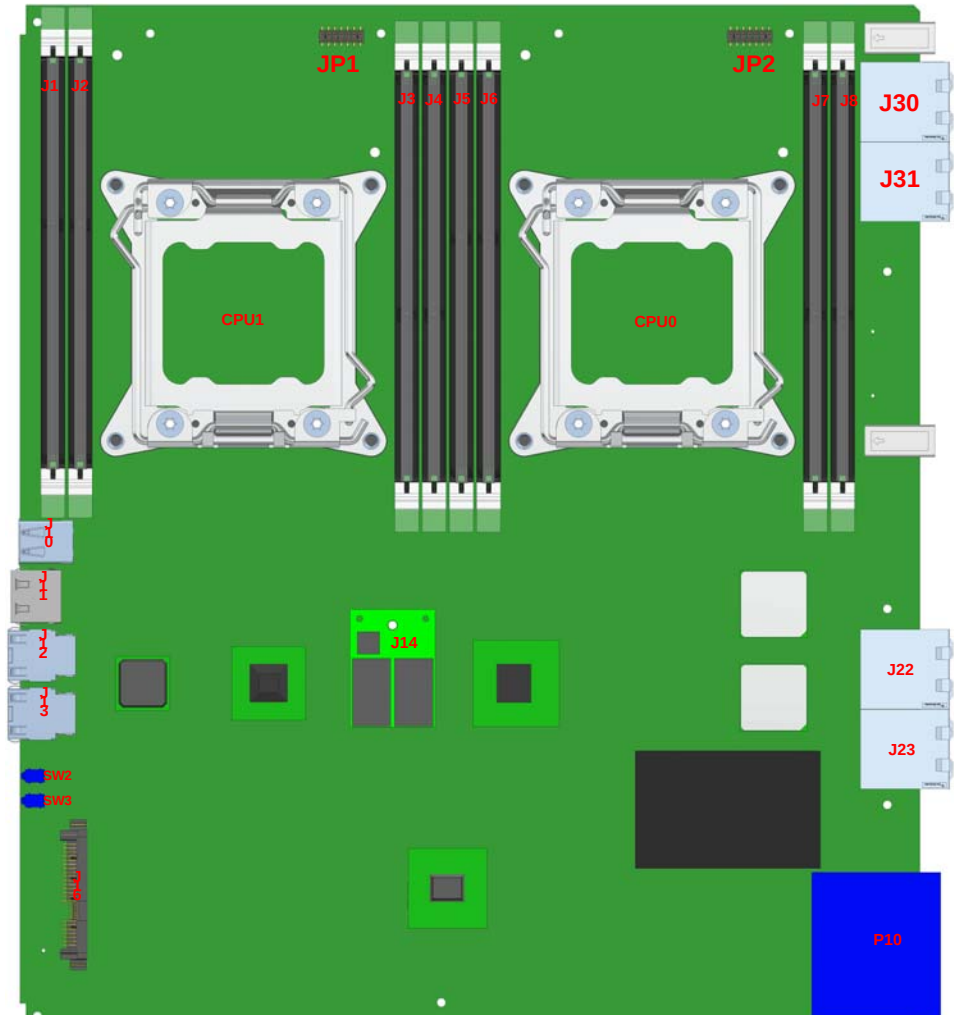
| | |
|---|---|
| On an anti-static plane, place the board so that you are facing the front plate connectors | |
| Remove the memory protection top cover. | |
| Insert the memory module into any available socket, aligning the notches on the module with the socket's key inserts. |  |
| 1- Insert the memory module in the connector using your thumbs.<br>2- Eject partially the memory module, using the connector latches while applying some pressure on the top to avoid the full removal of the modules.<br>3- Fully Reseat the modules in the connector using your thumbs.<br>4- Repeat steps 2 and 3 a second time.<br>5- Push down the memory module until the retaining clips lock on each side. |  |
| Repeat these steps to populate the other socket. | |
| To remove a memory module from a socket, push sideway the retaining clips on each side of the socket, to release the module. Pull out the memory from the socket. |  |

# 3.4 Onboard Connectors and Headers

Table 3-2:Onboard Connectors and Headers

| Description | Connector | Comments |
|---|---|---|
| Memory Sockets | J1 -J8 | DDR3 1333MHz or DDR3 1600 MHz Memory Sockets |
| USB Flash Connectors | J14 | USB Connectors for the USB SSD Modules |
| USB Connectors | J10 | Dual USB Connector |
| Management Console Port | J11 | RJ-45 Serial Port Connector |
| 1Gb/s RJ45 Connectors | J12 & J13 | Faceplate RJ45 Connectors |
| Base & Fabric Interface Connector | J23 & J23 | Base & Fabric Interface Connector |
| RTM Connectors | J30 & J31 | RTM Connectors |
| SAS HDD/SDD Connectors | J16 | Hard Disk Drive Connector |
| Power Connector | P10 | Power & IPMB |
| SW1 | Reset Switch | |
| SW2 | User Switch | |

Figure 3-2:Onboard Connectors and Headers Locations



# 3.5 Board Hot Swap and Installation

Because of the high-density pinout of the hard-metric connector, some precautions must be taken when connecting or disconnecting a board to/from a backplane:

1 Rail guides must be installed on the enclosure to slide the board to the backplane.

2 Do not force the board if there is mechanical resistance while inserting the board.

3 Once inserted, firmly attach the board to its enclosure using the 2 faceplate thumb-screws.

4 Use ejector handles to disconnect and extract the board from its enclosure.

**WARNING**

Always use a grounding wrist wrap when handling or removing the board from a chassis.

## 3.5.1 Installing the Board in the Chassis

To install a board in a chassis:

1 Remove the filler panel of the slot (see "Removing the Board").

2 Ensure the board is configured properly.

3 Carefully align the PCB edges in the bottom and top card guides.

4 Insert the board in the system and slide in until it makes contact with the backplane connectors.

5 Using both ejector handles, engage the board in the backplane connectors until both ejectors are locked.

6 Firmly attach the board to its enclosure using the 2 faceplate thumb-screws.

## 3.5.2 Removing the Board

To remove a board from a chassis:

1 Unscrew the top and the bottom faceplate thumb-screws.

2 Unlock the lower handle latch; this will initiate a clean shutdown of a properly configured operating system.

3 Wait until the blue LED is fully ON, this mean that the hot swap sequence is ready for board removal.

4 Use both ejectors to disengage the board from the backplane.

5 Slide the board out of the chassis.

### 3.5.3 Installing the RTM

To install the RTM:

1 Remove the filler panel of the slot.

2 Ensure the board is configured properly.

3 Carefully align the PCB edges in the bottom and top card guides.

4 Insert the board in the system and slide in until it makes contact with the CPU board.

5 Using both ejector handles, engage the board in the CPU board connectors until both ejectors are locked.

6 Firmly attach the board to its enclosure using the 2 faceplate thumb-screws.

### 3.5.4 Removing the RTM

To remove the RTM:

1 Unscrew the top and the bottom faceplate thumb-screws.

2 Unlock the lower handle latch.

3 Wait until the blue LED is fully ON, this mean that the hot swap sequence is ready for RTM removal.

4 Use both ejectors to disengage the board from the CPU board.

5 Slide the board out of the chassis.

## 3.6 Onboard SSD/HDD Approved List

Table 3-3:SSD/HDD Approved List

| Manufacturer Part Number | Description | Company |
|---|---|---|
| MTFDDAK480MAV-1AE12ABYY | SATA 480GB SSD 6Gb/s | Micron |
| MTFDDAK100MAR-1J1AA | SATA 100GB SSD 6Gb/s | Micron |
| SSDSA2CT040G3 | SATA 40GB SSD 3Gb/s | Intel |
| SSDSC2CW060A3 | SATA 60GB SSD 6Gb/s | Intel |
| SSDSC2CW120A3 | SATA 120GB SSD 6Gb/s | Intel |

*Chapter 4*

# Management


4.1 Hardware Management Overview ..... 27
4.2 Configuring LAN interface ..... 27
4.3 Web Management Interface ..... 27
4.4 Hardware Management Functionality ..... 30
4.5 IPMC Specific Features ..... 30
4.6 IPMC ..... 32

# 4. Management

## 4.1 Hardware Management Overview

The purpose of the hardware management system is to monitor, control, ensure proper operation and provide hot swap support for the ATCA board. The hardware management system watches over the basic health of the system, reports anomalies, and initiates corrective action when needed. The hardware management system can retrieve inventory information and sensor readings as well as receive event reports and failure notifications from boards and other Intelligent FRUs. The hardware management system can also perform basic recovery operations such as power cycle or reset of managed entities.

## 4.2 Configuring LAN interface

Before connecting to the Management Interface, the Management IP address needs to be set/confirmed. To obtain the address or configure it:

- Enter the BIOS Setup.
- Go to Set BMC network configuration menu, which is located under “Server Mgmt”.
- Choose the LAN channel to be configured.
- Select state and IP source (static or dynamic).
- When selecting IP source static, specify an IP Address, Subnet Mask and Gateway Address.
- Set LAN channel IP Address source, IP Address, Subnet Mask and if required, the Gateway address on the corresponding menu.

## 4.3 Web Management Interface

### 4.3.1 Connecting to the Web Management Interface

To access the Web Management Interface, at least one of the IPMC LAN interfaces must be configured and accessible over the Base interface.

To access the Web Management Interface:

- From a remote system on the base network, open a web browser.
- Type the IP address of the management controller in the browser.
- Default username and password are admin / admin.

**Note:**
A maximum of 4 sessions can be opened simultaneously. Up to 5 users can be configured.
An automatic logout will be done after 5 minutes of inactivity.

## 4.3.2 System

### 4.3.2.1 System Information

Once connected to the Web Management Interface, the first page displayed is the System Information. The current component versions and board information such as serial numbers and part numbers are displayed on this page

### 4.3.2.2 LAN Info

This page displays information on the IPMC LAN interfaces configuration. This configuration can be updated using this interface.

**Note:**
Modifying the configuration of the LAN interface being in use to access the Web Management Interface may lead to loss of connection.

### 4.3.2.3 System Tree

This page lists the IPMB addresses of the boards connected in the chassis.

## 4.3.3 Sensor

### 4.3.3.1 Reading

This page displays all board sensor readings. Values can be manually refreshed. Refer to Table 4-20 for a full list of sensors for this board.

## 4.3.4 Event Log

### 4.3.4.1 Reading

This page displays System Event Log (SEL) information and the event list. The SEL can have up to 5119 entries, and it can be cleared or refreshed manually. Events in the list may be browsed using the arrows under the table.

## 4.3.5 Control

### 4.3.5.1 Remote Power / Reset

This page displays the current Hot-Swap state, Power state and power level of the board and its managed FRUs. It also allows initiating a power down, graceful shutdown, power cycle, power up or reset of all the FRUs.

**Note:**
Power up of FRU0 is not supported, since the Web Management Interface is not accessible when FRU0 is powered down.

## 4.3.6 Maintenance

### *4.3.6.1 Component Info*

This page displays HPM Upgrade information and current component versions.

### *4.3.6.2 Component Upgrade*

This page allows upgrading the HPM bundle firmware from the Web Management Interface using a HPM file. To proceed, here are the steps to follow:

- Click “Browse...” and select the HPM file to upload. Then, click on “File Upload”.
- When the file is uploaded, information on the HPM file is displayed. At this point, it is possible to select individual components to upgrade if the file covers more than one component.
- Start the firmware upgrade by clicking “Start Upgrade Component(s)”. A progress bar will display the upgrade status for each component.
- If the upgrade is successful, the “Activate and Reboot Management” button will be displayed. Click on it to activate the new firmware.

### *4.3.6.3 Documentation*

This page includes the product "Quick Reference Sheet". Use the download button to save a copy of the PDF document.

### *4.3.6.4 Users*

This page is used to manage the authorized user accounts. A maximum of five (5) users can be configured. Each account can be enabled or disabled. Privilege levels are defined in the table below.

Table 4-1: Privilege Level Description

| Privilege Levels | Description |
|---|---|
| Administrator | All BMC commands are allowed, including modifying configuration settings. An Administrator can also execute configuration commands that would disable the channel that the Administrator is working on. |
| Operator | All BMC commands are allowed, except for modifying configuration settings which can change the behavior of the out-of-band interfaces. For example, Operator privilege does not allow the user to disable individual channels, or change user access privileges. |
| User | Only “basic” commands are allowed. These are primarily commands that read data and retrieve status. Commands that can be used to alter BMC configuration, write data to the management controllers, or perform system actions such as resets, power on/off, and watchdog activation are locked. |
| Callback | This may be considered the lowest privilege level. Only commands necessary to support initiating a callback are allowed. |
| No Access | No access is given to this user. |

The User ID 1 is a user without name and password. This user can be enabled or disabled and has a privilege level set to “User” by default.

The User ID2 is pre-configured as an admin user. It has “Administrator” privileges.

The User ID3 to User ID5 are configurable. These are disabled by default.

### 4.3.7 Logout

This button allows a safe logout of the management interface.

An automatic logout will be done after 5 minutes of inactivity.

## 4.4 Hardware Management Functionality

The Front Blade Unit supports an “intelligent” hardware management system, based on the Intelligent Platform Management Interface (IPMI) Specification. The hardware management system of the Front Blade Unit provides the ability to manage the power and interconnect needs of intelligent devices, to monitor events, and to log events to a central repository.

## 4.5 IPMC Specific Features

#### *4.5.0.1 IPMC - Interface*

The principal management-oriented link within a Shelf is a two-way redundant implementation of the Intelligent Platform Management Bus (IPMB). IPMB is based on the inter-integrated circuit (I2C) bus and is part of the IPMI architecture. In AdvancedTCA Shelves, the main IPMB is called IPMB-0. Each entity attached to IPMB-0 does so through an IPM Controller, the distributed management controller of the IPMI architecture. Shelf Managers attach to IPMB-0 through a variant IPM Controller called the Shelf Management Controller (ShMC). AdvancedTCA IPM Controllers, besides supporting dual redundant IPMBs, also have responsibility for detecting and recovering from IPMB faults.

The reliability of the AdvancedTCA IPMB-0 is increased by using two IPMBs, with the two IPMBs referenced as IPMB-A and IPMB-B. The aggregation of the two IPMBs is IPMB-0. The IPM Controllers aggregate the information received on both IPMBs. An IPM Controller that has a message ready for transmission selects which IPMB to transmit on in a round robin fashion; An IPM Controller tries to alternate the transmission of messages between IPMB-A and IPMB-B.

If an IPM Controller is unable to transmit on the desired IPMB then it tries to send the message on the alternate IPMB. By using this approach, an IPMB can become unavailable and then available without the IPM Controller needing to take specific action.

#### *4.5.0.2 IPMC - System Manager Interface*

The Section 24 of [IPMI 2.0] describes how IPMI messages can be sent to and from the IPMC encapsulated in RMCP (Remote Management Control Protocol) packet datagrams. This capability is also referred to as “IPMI over LAN” (IOL). IPMI also defines the associated LAN-specific configuration interfaces, as well as commands for discovering IPMI-based systems. The Distributed Management Task Force (DMTF) specifies the RMCP format. This LAN communication path makes the Front Blade Unit reachable by the System Manager for any management action (IPMC firmware upgrade, query of all FRU Data, CPU reset etc.) without the need to go through the ShMC.

#### 4.5.0.3 IPMC - System Event Log

The Kontron IPMC implementation includes a Local System Event Log device as specified in the Section 31 of [IPMI 2.0]. The local System Event Log is a nonvolatile repository for events generated by the front board and all managed FRUs (RTM, etc). The local SEL provides space for more than 5000 entries. However, even when events are logged into the local SEL, the IPMI platform event messages are still generated by the IPMC's Event Generator and sent to the centralized SEL hosted by the Shelf Manager through the IPMB-0 communication path - [PICMG 3.0] chapter 3.5; [IPMI 2.0] Section 29. The local SEL is useful for maintenance purposes and provides access to the events after the FRU has been extracted from the Shelf.

### 4.5.1 Sensors

For more details about onboard sensors consult the application note: AT8070 Sensor User Guide. This application note is available from the Kontron support site at: cbu.kontron.ca

# 4.6 IPMC

## 4.6.1 Supported Commands

The table below lists the IPMI commands supported by the IPMC. This table is identical to the one provided by PICMG 3.0. The last column indicates the AT8070's support for the specific command.

Table 4-2:IPM Device Supported Commands for IPMC

| | IPMI Spec. section | NetFn | CMD | IPMI BMC req. | Carrier IPMC req. | Kontron support on IPMC |
|---|---|---|---|---|---|---|
| IPM Device "Global" Commands | | | | M | M | |
| Get Device ID | 20.1 | App | 01h | M | M | Yes |
| Cold Reset | 20.2 | App | 02h | O | O | Yes |
| Warm Reset | 20.3 | App | 03h | O | O | No |
| Get Self Test Results | 20.4 | App | 04h | M | M | Yes |
| Manufacturing Test On | 20.5 | App | 05h | O | O | Yes |
| Set ACPI Power State | 20.6 | App | 06h | O | O | Yes |
| Get ACPI Power State | 20.7 | App | 07h | O | O | Yes |
| Get Device GUID | 20.8 | App | 08h | O | O | Yes |

Table 4-3:Watchdog Timer Supported Commands for IPMC

| | IPMI Spec. section | NetFn | CMD | IPMI BMC req. | Carrier IPMC req. | Kontron support on IPMC |
|---|---|---|---|---|---|---|
| BMC Watchdog Timer Commands | | | | M | M | |
| Reset Watchdog Timer | 27.5 | App | 22h | M | M | Yes |
| Set Watchdog Timer | 27.6 | App | 24h | M | M | Yes |
| Get Watchdog Timer | 27.7 | App | 25h | M | M | Yes |

Table 4-4:Device Messaging Supported Commands for IPMC

| | IPMI Spec. section | NetFn | CMD | IPMI BMC req. | Carrier IPMC req. | Kontron support on IPMC |
|---|---|---|---|---|---|---|
| BMC Device and Messaging Commands[5] | | | | M | O | |
| Set BMC Global Enables | 22.1 | App | 2Eh | M | O/M | Yes |
| Get BMC Global Enables | 22.2 | App | 2Fh | M | O/M | Yes |
| Clear Message Flags | 22.3 | App | 30h | M | O/M | Yes |
| Get Message Flags | 224 | App | 31h | M | O/M | Yes |

| | IPMI Spec. section | NetFn | CMD | IPMI BMC req. | Carrier IPMC req. | Kontron support on IPMC |
|---|---|---|---|---|---|---|
| Enable Message Channel Receive | 22.5 | App | 32h | O | O | Yes |
| Get Message | 22.6 | App | 33h | M | O/M | Yes |
| Send Message | 22.7 | App | 34h | M | M | Yes |
| Read Event Message Buffer | 22.8 | App | 35h | O | O | Yes |
| Get BT Interface Capabilities | 22.10 | App | 36h | M | O/M | No |
| Get System GUID | 22.14 | App | 37h | O | O | Yes |
| Get Channel Authentication Capabilities | 22.13 | App | 38h | O | O | Yes |
| Get Session Challenge | 22.15 | App | 39h | O | O | Yes |
| Activate Session | 22.17 | App | 3Ah | O | O | Yes |
| Set Session Privilege Level | 22.18 | App | 3Bh | O | O | Yes |
| Close Session | 22.19 | App | 3Ch | O | O | Yes |
| Get Session Info | 22.20 | App | 3Dh | O | O | Yes |
| Get AuthCode | 22.21 | App | 3Fh | O | O | No |
| Set Channel Access | 22.22 | App | 40h | O | O | Yes |
| Get Channel Access | 22.23 | App | 41h | O | O | Yes |
| Get Channel Info | 22.24 | App | 42h | O | O | Yes |
| Set User Access | 22.26 | App | 43h | O | O | Yes |
| Get User Access | 22.27 | App | 44h | O | O | Yes |
| Set User Name | 22.28 | App | 45h | O | O | Yes |
| Get User Name | 22.29 | App | 46h | O | O | Yes |
| Set User Password | 22.30 | App | 47h | O | O | Yes |
| Activate Payload | 24.1 | App | 48h | | | Yes |
| Deactivate Payload | 24.2 | App | 49h | | | Yes |
| Get Payload Activation Status | 24.4 | App | 4Ah | | | Yes |
| Get Payload Instance Info | 24.5 | App | 4Bh | | | Yes |
| Set User Payload Access | 24.6 | App | 4Ch | | | Yes |
| Get User Payload Access | 24.7 | App | 4Dh | | | Yes |
| Get Channel Payload Support | 24.8 | App | 4Eh | | | Yes |
| Get Channel Payload Version | 24.9 | App | 4Fh | | | Yes |
| Get Channel OEM Payload Info | 24.10 | App | 50h | | | No |
| Master Write-Read | 22.11 | App | 52h | | | Yes |

| | IPMI Spec. section | NetFn | CMD | IPMI BMC req. | Carrier IPMC req. | Kontron support on IPMC |
|---|---|---|---|---|---|---|
| Get Channel Cipher Suites | 22.15 | App | 54h | | | Yes |
| Suspend/Resume Payload Encryption | 24.3 | App | 55h | | | Yes |
| Set Channel Security Keys | 22.25 | App | 56h | | | No |
| Get System Interface Capabilities | 22.9 | App | 57h | | | Yes |

Table 4-5:Chassis Device Supported Commands for IPMC

| | IPMI Spec. section | NetFn | CMD | IPMI BMC req. | Carrier IPMC req. | Kontron support on IPMC |
|---|---|---|---|---|---|---|
| Chassis Device Commands | | | | O | O | |
| Get Chassis Capabilities | 28.1 | Chassis | 00h | M | O | Yes |
| Get Chassis Status | 28.2 | Chassis | 01h | O/M | O | Yes |
| Chassis Control | 28.3 | Chassis | 02h | O/M | O | Yes |
| Chassis Reset | 28.4 | Chassis | 03h | O | O | No |
| Chassis Identify | 28.5 | Chassis | 04h | O | O | No |
| Set Chassis Capabilities | 28.7 | Chassis | 05h | O | O | No |
| Set Power Restore Policy | 28.8 | Chassis | 06h | O | O | No |
| Get System Restart Cause | 28.11 | Chassis | 07h | O | O | No |
| Set System Boot Options | 28.12 | Chassis | 08h | | | No |
| Get System Boot Options | 28.13 | Chassis | 09h | | | No |
| Get POH Counter | 22.12 | Chassis | 0Fh | O | O | No |

Table 4-6:Event Supported Commands for IPMC

| | IPMI Spec. section | NetFn | CMD | IPMI BMC req. | Carrier IPMC req. | Kontron support on IPMC |
|---|---|---|---|---|---|---|
| Event Commands | | | | M | M | |
| Set Event Receiver | 29.1 | S/E | 01h | M | M | Yes |
| Get Event Receiver | 29.2 | S/E | 02h | M | M | Yes |
| Platform Event | 29.3 | S/E | 03h | M | M | Yes |

Table 4-7:PEF and Alerting Supported Commands for IPMC

| | IPMI Spec. section | NetFn | CMD | IPMI BMC req. | Carrier IPMC req. | Kontron support on IPMC |
|---|---|---|---|---|---|---|
| PEF and Alerting Commands | | | | O | O | |
| Get PEF Capabilities | 30.1 | S/E | 10h | M | M | Yes |
| Arm PEF Postpone Timer | 30.2 | S/E | 11h | M | M | Yes |
| Set PEF Configuration Parameters | 30.3 | S/E | 12h | M | M | Yes |
| Get PEF Configuration Parameters | 30.4 | S/E | 13h | M | M | Yes |
| Set Last Processed Event ID | 30.5 | S/E | 14h | M | M | Yes |
| Get Last Processed Event ID | 30.6 | S/E | 15h | M | M | Yes |
| Alert Immediate | 30.7 | S/E | 16h | O | O | No |
| PET Acknowledge | 30.8 | S/E | 17h | O | O | No |

Table 4-8:Sensor Device Supported Commands for IPMC

| | IPMI Spec. section | NetFn | CMD | IPMI BMC req. | Carrier IPMC req. | Kontron support on IPMC |
|---|---|---|---|---|---|---|
| Sensor Device Commands | | | | O | M | |
| Get Device SDR Info | 35.2 | S/E | 20h | O | M | Yes |
| Get Device SDR | 35.3 | S/E | 21h | O | M | Yes |
| Reserve Device SDR Repository | 35.4 | S/E | 22h | O | M | Yes |
| Get Sensor Reading Factors | 35.5 | S/E | 23h | O | M | No |
| Set Sensor Hysteresis | 35.6 | S/E | 24h | O | O | Yes |
| Get Sensor Hysteresis | 35.7 | S/E | 25h | O | O | Yes |
| Set Sensor Threshold | 35.8 | S/E | 26h | O | O | Yes |
| Get Sensor Threshold | 35.9 | S/E | 27h | O | O | Yes |
| Set Sensor Event Enable | 35.10 | S/E | 28h | O | O | Yes |
| Get Sensor Event Enable | 35.11 | S/E | 29h | O | O | Yes |
| Re-arm Sensor Events | 35.12 | S/E | 2Ah | O | O | No |
| Get Sensor Event Status | 35.13 | S/E | 2Bh | O | O | No |
| Get Sensor Reading | 35.14 | S/E | 2Dh | M | M | Yes |
| Set Sensor Type | 35.15 | S/E | 2Eh | O | O | No |
| Get Sensor Type | 35.16 | S/E | 2Fh | O | O | No |
| Set Sensor Reading and Event Status | 35.17 | S/E | 30h | O | O | Yes |

Table 4-9:FRU Device Supported Commands for IPMC

| | IPMI Spec. section | NetFn | CMD | IPMI BMC req. | Carrier IPMC req. | Kontron support on IPMC |
|---|---|---|---|---|---|---|
| FRU Device Commands | | | | M | M | |
| Get FRU Inventory Area Info | 34.1 | Storage | 10h | M | M | Yes |
| Read FRU Data | 34.2 | Storage | 11h | M | M | Yes |
| Write FRU Data | 34.3 | Storage | 12h | M | M | Yes |

Table 4-10:SDR Device Supported Commands for IPMC

| | IPMI Spec. section | NetFn | CMD | IPMI BMC req. | Carrier IPMC req. | Kontron support on IPMC |
|---|---|---|---|---|---|---|
| SDR Device Commands | | | | M | O | |
| Get SDR Repository Info | 33.9 | Storage | 20h | M | M | No |
| Get SDR Repository Allocation Info | 33.10 | Storage | 21h | O | O | No |
| Reserve SDR Repository | 33.11 | Storage | 22h | M | M | No |
| Get SDR | 33.12 | Storage | 23h | M | M | No |
| Add SDR | 33.13 | Storage | 24h | M | O/M | No |
| Partial Add SDR | 33.14 | Storage | 25h | M | O/M | No |
| Delete SDR | 33.15 | Storage | 26h | O | O | No |
| Clear SDR Repository | 33.16 | Storage | 27h | M | O/M | No |
| Get SDR Repository Time | 33.17 | Storage | 28h | O/M | O/M | No |
| Set SDR Repository Time | 33.18 | Storage | 29h | O/M | O/M | No |
| Enter SDR Repository Update Mode | 33.19 | Storage | 2Ah | O | O | No |
| Exit SDR Repository Update Mode | 33.20 | Storage | 2Bh | M | M | No |
| Run Initialization Agent | 33.21 | Storage | 2Ch | O | O | No |

Table 4-11:SEL Device Supported Commands for IPMC

| | IPMI Spec. section | NetFn | CMD | IPMI BMC req. | Carrier IPMC req. | Kontron support on IPMC |
|---|---|---|---|---|---|---|
| SEL Device Commands | | | | M | O | |
| Get SEL Info | 31.2 | Storage | 40h | M | M | Yes |
| Get SEL Allocation Info | 31.3 | Storage | 41h | O | O | Yes |
| Reserve SEL | 31.4 | Storage | 42h | O | O | Yes |
| Get SEL Entry | 31.5 | Storage | 43h | M | M | Yes |
| Add SEL Entry | 31.6 | Storage | 44h | M | M | Yes |
| Partial Add SEL Entry | 31.7 | Storage | 45h | M | M | No |
| Delete SEL Entry | 31.8 | Storage | 46h | O | O | Yes |

| | IPMI Spec. section | NetFn | CMD | IPMI BMC req. | Carrier IPMC req. | Kontron support on IPMC |
|---|---|---|---|---|---|---|
| Clear SEL | 31.9 | Storage | 47h | M | M | Yes |
| Get SEL Time | 31.10 | Storage | 48h | M | M | Yes |
| Set SEL Time | 31.11 | Storage | 49h | M | M | Yes |
| Get Auxiliary Log Status | 31.12 | Storage | 5Ah | O | O | No |
| Set Auxiliary Log Status | 31.13 | Storage | 5Bh | O | O | No |

Table 4-12:LAN Device Supported Commands for IPMC

| | IPMI Spec. section | NetFn | CMD | IPMI BMC req. | Carrier IPMC req. | Kontron support on IPMC |
|---|---|---|---|---|---|---|
| LAN Device Commands | | | | O | O | |
| Set LAN Configuration Parameters | 23.1 | Transport | 01h | O/M | O/M | Yes |
| Get LAN Configuration Parameters | 23.2 | Transport | 02h | O/M | O/M | Yes |
| Suspend BMC ARPs | 23.3 | Transport | 03h | O/M | O/M | Yes |
| Get IP/UDP/RMCP Statistics | 23.4 | Transport | 04h | O | O | Yes |

Table 4-13:Serial/Modem Device Supported Commands for IPMC

| | IPMI Spec. section | NetFn | CMD | IPMI BMC req. | Carrier IPMC req. | Kontron support on IPMC |
|---|---|---|---|---|---|---|
| Serial/Modem Device Commands | | | | O | O | |
| Set Serial/Modem Configuration | 25.1 | Transport | 10h | O/M | O/M | No |
| Get Serial/Modem Configuration | 25.2 | Transport | 11h | O/M | O/M | No |
| Set Serial/Modem Mux | 25.3 | Transport | 12h | O | O | No |
| Get TAP Response Codes | 25.4 | Transport | 13h | O | O | No |
| Set PPP UDP Proxy Transmit Data | 25.5 | Transport | 14h | O | O | No |
| Get PPP UDP Proxy Transmit Data | 25.6 | Transport | 15h | O | O | No |
| Send PPP UDP Proxy Packet | 25.7 | Transport | 16h | O | O | No |
| Get PPP UDP Proxy Receive Data | 25.8 | Transport | 17h | O | O | No |

| | IPMI Spec. section | NetFn | CMD | IPMI BMC req. | Carrier IPMC req. | Kontron support on IPMC |
|---|---|---|---|---|---|---|
| Serial/Modem Connection Active | 25.9 | Transport | 18h | O/M | O/M | No |
| Callback | 25.10 | Transport | 19h | O | O | No |
| Set User Callback Options | 25.11 | Transport | 1Ah | O | O | No |
| Get User Callback Options | 25.12 | Transport | 1Bh | O | O | No |

Table 4-14:SOL Commands

| | IPMI Spec. section | NetFn | CMD | IPMI BMC req. | Carrier IPMC req. | Kontron support on IPMC |
|---|---|---|---|---|---|---|
| SOL Commands | | | | O | O | |
| SOL Activating | 26.1 | Transport | | 20h | | Yes |
| Set SOL Configuration Params | 26.2 | Transport | | 21h | | Yes |
| Get SOL Configuration Params | 26.3 | Transport | | 22h | | Yes |

Table 4-15:PICMG 3.0 Commands for IPMC

| | IPMI Spec. section | NetFn | CMD | IPMI BMC req. | Carrier IPMC req. | Kontron support on IPMC |
|---|---|---|---|---|---|---|
| AdvancedTCA® | PICMG® 3.0 Table | | | | M | |
| Get PICMG Properties | 3-11 | PICMG | 00h | | M | Yes |
| Get Address Info | 3-10 | PICMG | 01h | | M | Yes |
| Get Shelf Address Info | 3-16 | PICMG | 02h | | O | Yes |
| Set Shelf Address Info | 3-17 | PICMG | 03h | | O | No |
| FRU Control | 3-27 | PICMG | 04h | | M | Yes |
| Get FRU LED Properties | 3-29 | PICMG | 05h | | M | Yes |
| Get LED Color Capabilities | 3-30 | PICMG | 06h | | M | Yes |
| Set FRU LED State | 3-31 | PICMG | 07h | | M | Yes |
| Get FRU LED State | 3-32 | PICMG | 08h | | M | Yes |
| Set IPMB State | 3-70 | PICMG | 09h | | M | Yes |
| Set FRU Activation Policy | 3-20 | PICMG | 0Ah | | M | Yes |
| Get FRU Activation Policy | 3-21 | PICMG | 0Bh | | M | Yes |
| Set FRU Activation | 3-19 | PICMG | 0Ch | | M | Yes |
| Get Device Locator Record ID | 3-39 | PICMG | 0Dh | | M | Yes |
| Set Port State | 3-59 | PICMG | 0Eh | | O/M | Yes |
| Get Port State | 3-60 | PICMG | 0Fh | | O/M | Yes |

| | IPMI Spec. section | NetFn | CMD | IPMI BMC req. | Carrier IPMC req. | Kontron support on IPMC |
|---|---|---|---|---|---|---|
| Compute Power Properties | 3-82 | PICMG | 10h | | M | Yes |
| Set Power Level | 3-84 | PICMG | 11h | | M | Yes |
| Get Power Level | 3-83 | PICMG | 12h | | M | Yes |
| Renegotiate Power | 3-91 | PICMG | 13h | | O | No |
| Get Fan Speed Properties | 3-86 | PICMG | 14h | | O/M | No |
| Set Fan Level | 3-88 | PICMG | 15h | | O/M | No |
| Get Fan Level | 3-87 | PICMG | 16h | | O/M | No |
| Bused Resource | 3-62 | PICMG | 17h | | O/M | No |
| Get IPMB Link Info | 3-68 | PICMG | 18h | | O/M | Yes |
| Get Shelf Manager IPMB Address | 3-38 | PICMG | 1Bh | | M | No |
| Set Fan Policy | 3-89 | PICMG | 1Ch | | M | No |
| Get Fan Policy | 3-90 | PICMG | 1Dh | | M | No |
| FRU Control Capabilities | 3-29 | PICMG | 1Eh | | M | Yes |
| FRU Inventory Device Lock Control | 3-42 | PICMG | 1Fh | | M | No |
| FRU Inventory Device Write | 3-43 | PICMG | 20h | | M | No |
| Get Shelf Manager IP Addresses | 3-36 | PICMG | 21h | | M | No |
| Get Shelf Power Allocation | 3-85 | PICMG | 22h | | M | No |
| Get Telco Alarm Capability | 3-93 | PICMG | 29h | | O/M | No |
| Set Telco Alarm State | 3-94 | PICMG | 2Ah | | O/M | No |
| Get Telco Alarm State | 3-95 | PICMG | 2Bh | | O/M | No |
| Get Telco Alarm Location | 3-95 | PICMG | 39h | | O/M | No |
| Set FRU Extracted | 3-25 | PICMG | 3Ah | | M | No |

Table 4-16:HPM Commands

| | IPMI Spec. section | NetFn | CMD | IPMI BMC req. | Carrier IPMC req. | Kontron support on IPMC |
|---|---|---|---|---|---|---|
| HPM | | | | | | |
| Get target upgrade capabilities | 3-3 | PICMG | 2Eh | | M | Yes |
| Get component properties | 3-5 | PICMG | 2Fh | | | Yes |
| Abort Firmware Upgrade | 3-15 | PICMG | 30h | | O | Yes |
| Initiate upgrade action | 3-8 | PICMG | 31h | | M[1] | Yes |
| Upload firmware block | 3-9 | PICMG | 32h | | M | Yes |
| Finish firmware upload | 3-10 | PICMG | 33h | | M | Yes |
| Get upgrade status | 3-2 | PICMG | 34h | | O/M[2] | Yes |

| | IPMI Spec. section | NetFn | CMD | IPMI BMC req. | Carrier IPMC req. | Kontron support on IPMC |
|---|---|---|---|---|---|---|
| Activate firmware | 3-11 | PICMG | 35h | | M | Yes |
| Query self-test results | 3-12 | PICMG | 36h | | O/M[3] | Yes |
| Query Rollback status | 3-13 | PICMG | 37h | | O/M[4] | Yes |
| Initiate Manual Rollback | 3-14 | PICMG | 38h | | O/M[5] | Yes |

## 4.6.2 Sensor Data Records

Information that describes the IPMC capabilities is provided through two mechanisms: capabilities commands and Sensor Data Records (SDRs). Capabilities commands are commands within the IPMI command set that return fields providing information on other commands and functions the controller can handle.

Sensor Data Records are data records containing information about the type and number of sensors in the platform, sensor threshold support, event generation capabilities, and information on what types of readings the sensor provides. The primary purpose of Sensor Data Records is to describe the sensor configuration of the hardware management subsystem.

IPMCs are required to maintain Device Sensor Data Records for the sensors and objects they manage. Access methods for the Device SDR entries are described in the [IPMI 2.0] specification, Section 35, "Sensor Device Commands."

After a FRU is inserted, the System Manager, using the Shelf Manager, may gather the various SDRs from the FRUs' IPM Controllers to discover the various objects and how to use them. The System Manager uses the "Sensor Device Commands" to gather this information. Thus, commands, such as "Get Device SDR Info" and "Get Device SDR," which are optional in the IPMI specification, are mandatory in AdvancedTCA systems.

Most of the current Shelf Manager implementations gathers the individual Device Sensor Data Records of each FRU into a centralized SDR Repository. This SDR Repository may exist in either the Shelf Manager or System Manager. If the Shelf Manager implements the SDR Repository on-board, it shall also respond to "SDR Repository" commands.

This duplication of SDR repository commands can create some confusion among AdvancedTCA users. It is mandatory for IPMC to support the Sensor Device Commands for IPMC built-in SDR as described in the [IPMI 2.0] specification, Section 35, "Sensor Device Commands." For the ShMC, the same set of commands for the centralized SDR Repository must be supported but they are described in the [IPMI 2.0] specification, Section 33, "SDR Repository Commands."

### *4.6.2.1 IPMC Sensors*

Table 4-17: IPMC Sensors

| Sensor ID | Sensor Name | Type | Description |
|---|---|---|---|
| 0 | FRU0 Hot Swap | Discrete | ATCA Board FRU Hot Swap Sensor for FRU 0 (Front Board)<br>Sensor type code = F0h PICMG Hot Swap<br>Event Reading type code = 6Fh Sensor specific<br>See PICMG 3.0 R3.0 Table 3-22, "FRU Hot Swap event message" |
| 1 | FRU1 Hot Swap | Discrete | ATCA Board FRU Hot Swap Sensor for FRU 1 (RTM)<br>Available only when RTM is inserted<br>Sensor type code = F0h PICMG Hot Swap<br>Event Reading type code = 6Fh Sensor specific<br>See PICMG 3.0 R3.0 Table 3-22, "FRU Hot Swap event message" |
| 2 | FRU2 Hot Swap | Discrete | ATCA Board FRU Hot Swap Sensor for FRU 2 (RTM Disk 1)<br>Available only when RTM and 1 disk is inserted<br>Sensor type code = F0h PICMG Hot Swap<br>Event Reading type code = 6Fh Sensor specific<br>See PICMG 3.0 R3.0 Table 3-22, "FRU Hot Swap event message" |
| 3 | FRU3 Hot Swap | Discrete | ATCA Board FRU Hot Swap Sensor for FRU 3 (RTM Disk 2)<br>Available only when RTM and 2 disks are inserted<br>Sensor type code = F0h PICMG Hot Swap<br>Event Reading type code = 6Fh Sensor specific<br>See PICMG 3.0 R3.0 Table 3-22, "FRU Hot Swap event message" |
| 5 | FRU0 Reconfig | Discrete | Sensor Population Change on Carrier<br>Sensor type = 12h System Event<br>Event Reading type code = 6Fh Sensor specific, only offset 0 is used<br>See AMC.0 R2.0 for event trigger<br>See IPMI v2.0 table 42-3, Sensor type code 12h for sensor definition |
| 6 | Temp Board Inlet | Threshold | Board Inlet Temperature (Degrees)<br>Sensor type = 01h temperature<br>Event Reading type code = 01h threshold based<br>See IPMI v2.0 table 42-2 for threshold based event |
| 8 | Temp CPU0 | Threshold | CPU0 Temperature (Degrees)<br>Sensor type = 01h temperature<br>Event Reading type code = 01h threshold based<br>See IPMI v2.0 table 42-2 for threshold based event |
| 9 | Temp CPU1 | Threshold | CPU1 Temperature (Degrees)<br>Sensor type = 01h temperature<br>Event Reading type code = 01h threshold based<br>See IPMI v2.0 table 42-2 for threshold based event |

| Sensor ID | Sensor Name | Type | Description |
|---|---|---|---|
| 10 | Temp Vcore0 | Threshold | CPU0 Vcore Switcher Temperature (Degrees)<br>Sensor type = 01h temperature<br>Event Reading type code = 01h threshold based<br>See IPMI v2.0 table 42-2 for threshold based event |
| 11 | Temp Vcore1 | Threshold | CPU1 Vcore Switcher Temperature (Degrees)<br>Sensor type = 01h temperature<br>Event Reading type code = 01h threshold based<br>See IPMI v2.0 table 42-2 for threshold based event |
| 12 | Temp DIMM A | Threshold | DIMM A Temperature (Degrees)<br>Sensor type = 01h temperature<br>Event Reading type code = 01h threshold based<br>See IPMI v2.0 table 42-2 for threshold based event |
| 13 | Temp DIMM B | Threshold | DIMM B Temperature (Degrees)<br>Sensor type = 01h temperature<br>Event Reading type code = 01h threshold based<br>See IPMI v2.0 table 42-2 for threshold based event |
| 14 | Temp DIMM C | Threshold | DIMM C Temperature (Degrees)<br>Sensor type = 01h temperature<br>Event Reading type code = 01h threshold based<br>See IPMI v2.0 table 42-2 for threshold based event |
| 15 | Temp DIMM D | Threshold | DIMM D Temperature (Degrees)<br>Sensor type = 01h temperature<br>Event Reading type code = 01h threshold based<br>See IPMI v2.0 table 42-2 for threshold based event |
| 16 | Temp DIMM E | Threshold | DIMM E Temperature (Degrees)<br>Sensor type = 01h temperature<br>Event Reading type code = 01h threshold based<br>See IPMI v2.0 table 42-2 for threshold based event |
| 17 | Temp DIMM F | Threshold | DIMM F Temperature (Degrees)<br>Sensor type = 01h temperature<br>Event Reading type code = 01h threshold based<br>See IPMI v2.0 table 42-2 for threshold based event |
| 18 | Temp DIMM G | Threshold | DIMM G Temperature (Degrees)<br>Sensor type = 01h temperature<br>Event Reading type code = 01h threshold based<br>See IPMI v2.0 table 42-2 for threshold based event |
| 19 | Temp DIMM H | Threshold | DIMM H Temperature (Degrees)<br>Sensor type = 01h temperature<br>Event Reading type code = 01h threshold based<br>See IPMI v2.0 table 42-2 for threshold based event |

| Sensor ID | Sensor Name | Type | Description |
|---|---|---|---|
| 20 | Temp Disk | Threshold | Disk Temperature (Degrees)<br>Sensor type = 01h temperature<br>Event Reading type code = 01h threshold based<br>See IPMI v2.0 table 42-2 for threshold based event |
| 21 | Temp Disk1 | Threshold | Disk 1 Temperature (Degrees)<br>Available only when RTM 5707 and at least 1 disk is inserted<br>Sensor type = 01h temperature<br>Event Reading type code = 01h threshold based<br>See IPMI v2.0 table 42-2 for threshold based event |
| 22 | Temp Disk2 | Threshold | Disk 2 Temperature (Degrees)<br>Available only when RTM 5707 and at least 1 disk is inserted<br>Sensor type = 01h temperature<br>Event Reading type code = 01h threshold based<br>See IPMI v2.0 table 42-2 for threshold based event |
| 23 | Brd Input Power | Threshold | Power consumption in watts of the complete blade (including managed FRU) Sensor type = 0Bh Other Unit-Based Sensor (Watt)<br>Event Reading type code = 01h threshold base<br>See IPMI v2.0 table 42-2 for threshold based event |
| 24 | FRU0 Brd Power | Threshold | FRU 0 (ATCA Board) Power consumption in watts<br>Sensor type = 0Bh Other Unit-Based Sensor (Watt)<br>Event Reading type code = 01h threshold base<br>See IPMI v2.0 table 42-2 for threshold based event |
| 26 | FRU1 RTM Power | Threshold | FRU 1 (RTM) + FRU 2 (RTM's disk 1) + FRU 4 (RTM's disk 2) Power consumption in watts<br>Sensor type = 0Bh Other Unit-Based Sensor (Watt)<br>Event Reading type code = 01h threshold base<br>See IPMI v2.0 table 42-2 for threshold based event |
| 27 | Vcc -48V Feed | Threshold | Voltage on -48v feed board input power supply (Volts)<br>Sensor type = 02h voltage<br>Event Reading type code = 01h threshold based<br>See IPMI v2.0 table 42-2 for threshold based event |
| 28 | Vcc +12V SUS | Threshold | Voltage on 12V suspend (management) power supply<br>Sensor type = 02h voltage<br>Event Reading type code = 01h threshold based<br>See IPMI v2.0 table 42-2 for threshold based event |
| 29 | Vcc +5V SUS | Threshold | Voltage on board 5.0V suspend (management) power supply<br>Sensor type = 02h voltage<br>Event Reading type code = 01h threshold based<br>See IPMI v2.0 table 42-2 for threshold based event |

| Sensor ID | Sensor Name | Type | Description |
|---|---|---|---|
| 30 | Vcc +3.3V SUS | Threshold | Voltage on board 3.3V suspend (management) power supply (Volts)<br>Sensor type = 02h voltage<br>Event Reading type code = 01h threshold based<br>See IPMI v2.0 table 42-2 for threshold based event |
| 31 | Vcc +1.8V SUS | Threshold | Voltage on board 1.8V suspend (management) power supply (Volts)<br>Sensor type = 02h voltage<br>Event Reading type code = 01h threshold based<br>See IPMI v2.0 table 42-2 for threshold based event |
| 32 | Vcc +1.5V SUS | Threshold | Voltage on board 1.5V suspend (management) power supply (Volts)<br>Sensor type = 02h voltage<br>Event Reading type code = 01h threshold based<br>See IPMI v2.0 table 42-2 for threshold based event |
| 33 | Vcc +1.25V SUS | Threshold | Voltage on board 1.25V suspend (management) power supply (Volts)<br>Sensor type = 02h voltage<br>Event Reading type code = 01h threshold based<br>See IPMI v2.0 table 42-2 for threshold based event |
| 34 | Vcc +1.2V SUS | Threshold | Voltage on board 1.2V suspend (management) power supply (Volts)<br>Sensor type = 02h voltage<br>Event Reading type code = 01h threshold based<br>See IPMI v2.0 table 42-2 for threshold based event |
| 35 | Vcc +1.0V SUS | Threshold | Voltage on board 1.0V suspend (management) power supply (Volts)<br>Sensor type = 02h voltage<br>Event Reading type code = 01h threshold based<br>See IPMI v2.0 table 42-2 for threshold based event |
| 36 | Vcc +0.75V SUS | Threshold | Voltage on board 0.75V suspend (management) power supply (Volts)<br>Sensor type = 02h voltage<br>Event Reading type code = 01h threshold based<br>See IPMI v2.0 table 42-2 for threshold based event |
| 37 | Vcc +1.5V | Threshold | Voltage on board 1.5V payload power supply (Volts)<br>Sensor type = 02h voltage<br>Event Reading type code = 01h threshold based<br>See IPMI v2.0 table 42-2 for threshold based event |

| Sensor ID | Sensor Name | Type | Description |
|---|---|---|---|
| 38 | Vcc +1.2V | Threshold | Voltage on board 1.2V payload power supply (Volts)<br>Sensor type = 02h voltage<br>Event Reading type code = 01h threshold based<br>See IPMI v2.0 table 42-2 for threshold based event |
| 39 | Vcc +1.1V ME | Threshold | Voltage on board 1.1V payload power supply (Volts)<br>Sensor type = 02h voltage<br>Event Reading type code = 01h threshold based<br>See IPMI v2.0 table 42-2 for threshold based event |
| 40 | Vcc +1.0V A | Threshold | Voltage on board 1.0V A payload power supply (volts)<br>Sensor type = 02h voltage<br>Event Reading type code = 01h threshold based<br>See IPMI v2.0 table 42-2 for threshold based event40 |
| 41 | Vcc VCORE 0 | Threshold | Voltage on board CPU0 Vcore payload power supply (Volts)<br>Sensor type = 02h voltage<br>Event Reading type code = 01h threshold based<br>See IPMI v2.0 table 42-2 for threshold based event |
| 42 | Vcc VTT CPU 0 | Threshold | Voltage on board CPU0 VTT payload power supply (Volts)<br>Sensor type = 02h voltage<br>Event Reading type code = 01h threshold based<br>See IPMI v2.0 table 42-2 for threshold based event |
| 43 | Vcc VDDQ CPU 0 | Threshold | Voltage on board CPU0 VDDQ payload power supply (Volts)<br>Sensor type = 02h voltage<br>Event Reading type code = 01h threshold based<br>See IPMI v2.0 table 42-2 for threshold based event |
| 44 | Vcc VSA CPU 0 | Threshold | Voltage on board CPU0 VSA payload power supply (Volts)<br>Sensor type = 02h voltage<br>Event Reading type code = 01h threshold based<br>See IPMI v2.0 table 42-2 for threshold based event |
| 45 | Vcc PLL CPU 0 | Threshold | Voltage on board CPU0 PLL payload power supply (Volts)<br>Sensor type = 02h voltage<br>Event Reading type code = 01h threshold based<br>See IPMI v2.0 table 42-2 for threshold based event |
| 46 | Vcc VCORE 1 | Threshold | Voltage on board CPU1 Vcore payload power supply (Volts)<br>Sensor type = 02h voltage<br>Event Reading type code = 01h threshold based<br>See IPMI v2.0 table 42-2 for threshold based event |
| 47 | Vcc VTT CPU 1 | Threshold | Voltage on board CPU1 VTT payload power supply (Volts)<br>Sensor type = 02h voltage<br>Event Reading type code = 01h threshold based<br>See IPMI v2.0 table 42-2 for threshold based event |

| Sensor ID | Sensor Name | Type | Description |
|---|---|---|---|
| 48 | Vcc VDDQ CPU 1 | Threshold | Voltage on board CPU1 VDDQ payload power supply (Volts)<br>Sensor type = 02h voltage<br>Event Reading type code = 01h threshold based<br>See IPMI v2.0 table 42-2 for threshold based event |
| 49 | Vcc VSA CPU 1 | Threshold | Voltage on board CPU1 VSA payload power supply (Volts)<br>Sensor type = 02h voltage<br>Event Reading type code = 01h threshold based<br>See IPMI v2.0 table 42-2 for threshold based event |
| 50 | Vcc PLL CPU 1 | Discrete | Voltage on board CPU1 VSA payload power supply (Volts)<br>Sensor type = 02h voltage<br>Event Reading type code = 01h threshold based<br>See IPMI v2.0 table 42-2 for threshold based event |
| 51 | Fuse-Pres A Feed | Discrete | Fuse presence and fault detection -48 V on supply A<br>Sensor type = 08h Power Supply<br>Event Reading type code = 6Fh Sensor specific<br>only offset 0,1 are used<br>See IPMI v2.0 table 42-3, Sensor type code 08h for sensor definition |
| 52 | Fuse-Pres B Feed | Discrete | Fuse presence and fault detection -48 V on supply B<br>Sensor type = 08h Power Supply<br>Event Reading type code = 6Fh Sensor specific<br>only offset 0,1 are used<br>See IPMI v2.0 table 42-3, Sensor type code 08h for sensor definition |
| 53 | Power State | Discrete | Board Power State<br>Sensor type = D0h Kontron OEM Power State Sensor<br>Event Reading type code = 6Fh Sensor specific<br>See OEM sensor table, Sensor type code D1h for sensor definition |
| 54 | Power Good | Discrete | Actual power good status<br>Sensor type = 08h Power Supply<br>Event Reading type code = 77h OEM<br>See OEM sensor table, Event/Reading type code 77h for sensor definition |
| 55 | Power Good Event | Discrete | Power good status event that occur since the last power on or reset<br>Sensor type = 08h Power Supply<br>Event Reading type code = 77h OEM<br>See OEM sensor table, Event/Reading type code 77h for sensor definition |

| Sensor ID | Sensor Name | Type | Description |
|---|---|---|---|
| 56 | Board Reset | Discrete | Board reset type and sources<br>Sensor type = CFh OEM (Kontron Reset Sensor)<br>Event Reading type code = 03h Digital Discrete<br>Only offset 0,1 are used<br>See OEM sensor table, Sensor type code CFh for sensor definition |
| 57 | POST Value | Discrete | Show current postcode value. No event generated by this sensor<br>Sensor type = C6h OEM (Kontron POST value sensor)<br>Event Reading type code = 6Fh Sensor specific<br>Only offset 0 to 7 and 14 are used<br>See OEM sensor table, Sensor type code C6h for sensor definition |
| 58 | Memory Err | Discrete | Memory Error<br>Sensor type = 0Ch Memory<br>Event Reading type code = 6Fh Sensor specific<br>Only offset 0,1,7 are used<br>See IPMI v2.0 table 42-3, Sensor type code 0Ch for sensor definition |
| 59 | DIMM A Status | Discrete | DIMM A Status & Presence<br>Sensor type = 25h Entity Presence<br>Event Reading type code = 6Fh Sensor specific<br>Only offset 0,1,4,5,6,7 are used<br>See IPMI v2.0 table 42-3, Sensor type 25h (Entity Presence) for sensor definition |
| 60 | DIMM B Status | Discrete | DIMM B Status & Presence<br>Sensor type = 25h Entity Presence<br>Event Reading type code = 6Fh Sensor specific<br>Only offset 0,1,4,5,6,7 are used<br>See IPMI v2.0 table 42-3, Sensor type 25h (Entity Presence) for sensor definition |
| 61 | DIMM C Status | Discrete | DIMM C Status & Presence<br>Sensor type = 25h Entity Presence<br>Event Reading type code = 6Fh Sensor specific<br>Only offset 0,1,4,5,6,7 are used<br>See IPMI v2.0 table 42-3, Sensor type 25h (Entity Presence) for sensor definition |

| Sensor ID | Sensor Name | Type | Description |
|---|---|---|---|
| 62 | DIMM D Status | Discrete | DIMM D Status & Presence<br>Sensor type = 25h Entity Presence<br>Event Reading type code = 6Fh Sensor specific<br>Only offset0,1,4,5,6,7 are used<br>See IPMI v2.0 table 42-3, Sensor type 25h (Entity Presence) for sensor definition |
| 63 | DIMM E Status | Discrete | DIMM E Status & Presence<br>Sensor type = 25h Entity Presence<br>Event Reading type code = 6Fh Sensor specific<br>Only offset0,1,4,5,6,7 are used<br>See IPMI v2.0 table 42-3, Sensor type 25h (Entity Presence) for sensor definition |
| 64 | DIMM F Status | Discrete | DIMM F Status & Presence<br>Sensor type = 25h Entity Presence<br>Event Reading type code = 6Fh Sensor specific<br>Only offset 0,1,4,5,6,7 are used<br>See IPMI v2.0 table 42-3, Sensor type 25h (Entity Presence) for sensor definition |
| 65 | DIMM G Status | Discrete | DIMM G Status & Presence<br>Sensor type = 25h Entity Presence<br>Event Reading type code = 6Fh Sensor specific<br>Only offset 0,1,4,5,6,7 are used<br>See IPMI v2.0 table 42-3, Sensor type 25h (Entity Presence) for sensor definition |
| 66 | DIMM H Status | Discrete | DIMM H Status & Presence<br>Sensor type = 25h Entity Presence<br>Event Reading type code = 6Fh Sensor specific<br>Only offset 0,1 are used<br>See IPMI v2.0 table 42-3, Sensor type 25h (Entity Presence) for sensor definition |
| 67 | Memory Resize | Discrete | POST Memory Resize<br>Indicates if CMOS memory size has changed<br>Sensor type = 0Eh, POST Memory Resize<br>Event Reading type code = 03h Digital Discrete<br>Only offset 0,1 are used<br>See IPMI v2.0 table 42-3, Event/Reading type code 0Eh for sensor definition |

| Sensor ID | Sensor Name | Type | Description |
|---|---|---|---|
| 68 | Boot Error | Discrete | Boot Error<br>Sensor Type = 1Eh Boot Error<br>Reading type code = 6Fh Sensor Specific<br>Only offset 0 is used<br>See IPMI v2.0 table 42-3, Sensor type code 1Eh for sensor definition |
| 69 | CMOS Passwd | Discrete | CMOS Password Failure<br>Sensor type = 06h Platform Security Violation Attempt<br>Event Reading type code = 6Fh Sensor Specific<br>Only offset 1 and 4 are used<br>See IPMI v2.0 table 42-3, Sensor type code 06h for sensor definition |
| 70 | PCIe Error | Discrete | General PCIe Error<br>Sensor type = 13h Critical Interrupt<br>Event Reading type code = 6Fh Sensor Specific<br>Only offset 7 and 8 are used<br>See IPMI v2.0 table 42-3, Sensor type code 13h for sensor definition |
| 71 | PCIe RTM Error | Discrete | RTM PCIe Error<br>Sensor type = 13h Critical Interrupt<br>Event Reading type code = 6Fh Sensor Specific<br>Only offset 7 and 8 are used<br>See IPMI v2.0 table 42-3, Sensor type code 13h for sensor definition |
| 72 | PCIe BI Error | Discrete | Base Interface PCIe Error<br>Sensor type = 13h Critical Interrupt<br>Event Reading type code = 6Fh Sensor Specific<br>Only offset 7 and 8 are used<br>See IPMI v2.0 table 42-3, Sensor type code 13h for sensor definition |
| 73 | PCIe FI 0 Error | Discrete | Fabric Interface PCIe Error<br>Sensor type = 13h Critical Interrupt<br>Event Reading type code = 6Fh Sensor Specific<br>Only offset 7 and 8 are used<br>See IPMI v2.0 table 42-3, Sensor type code 13h for sensor definition |

| Sensor ID | Sensor Name | Type | Description |
|---|---|---|---|
| 74 | PCIe FI 1 Error | Discrete | Fabric Interface PCIe Error<br>Sensor type = 13h Critical Interrupt<br>Event Reading type code = 6Fh Sensor Specific<br>Only offset 7 and 8 are used<br>See IPMI v2.0 table 42-3, Sensor type code 13h for sensor definition |
| 75 | PCIe MI Error | Discrete | Management Interface PCIe Error<br>Sensor type = 13h Critical Interrupt<br>Event Reading type code = 6Fh Sensor Specific<br>Only offset 7 and 8 are used<br>See IPMI v2.0 table 42-3, Sensor type code 13h for sensor definition |
| 76 | Bios Flash 0 | Discrete | Bios Flash 0<br>Sensor type = 1Eh Boot Error<br>Event Reading type code = 6Fh Sensor Specific<br>Only offset 3 is used<br>See IPMI v2.0 table 42-3, Sensor type code 1Eh for sensor definition |
| 77 | Bios Flash 1 | Discrete | Bios Flash 1<br>Sensor type = 1Eh Boot Error<br>Event Reading type code = 6Fh Sensor Specific<br>Only offset 3 is used<br>See IPMI v2.0 table 42-3, Sensor type code 1Eh for sensor definition |
| 78 | ACPI State | Discrete | Advance Configuration and Power Interface State<br>Sensor type = 22h System ACPI Power State<br>Event Reading type code = 6Fh Sensor specific<br>Only offset 0,4,5,10,11,12,14 are used.<br>See IPMI v2.0 table 42-3, Sensor type code 22h (ACPI Power State) for sensor definition |
| 79 | IPMI Watchdog | Discrete | IPMI Watchdog (payload watchdog)<br>Sensor type = 23h Watchdog 2<br>Event Reading type code = 6Fh Sensor specific<br>Only offset 0,1,2,3,8 are used<br>See IPMI v2.0 table 42-3, Sensor type code 23h (Watchdog 2) for sensor definition |

| Sensor ID | Sensor Name | Type | Description |
|---|---|---|---|
| 80 | Health Error | Discrete | General health status, Aggregation of critical sensor<br>This list is flexible and could be adjust based on customer requirements<br>Sensor type = 24h Platform Alert<br>Event Reading type code = 03h Digital Discrete<br>Only offset 0,1 are used<br>See IPMI v2.0 table 42-3, Sensor type code 24h for sensor definition |
| 81 | IPMB0 Link State | Discrete | IPMB-0 fault detection sensor<br>Sensor type = F1h PICMG Physical IPMB-0<br>Event Reading type code = 6Fh Sensor specific<br>See PICMG 3.0 R3.0 Table 3-69, “Physical IPMB-0 event message” |
| 82 | FRU0 IPMBL State | Discrete | IPMB-L branch from FRU0 fault detection sensor<br>Sensor type = C3h OEM (Kontron OEM IPMB-L link state)<br>Event Reading type code = 6Fh Sensor specific<br>Only offset 2 and 3 are used<br>See OEM table, Sensor type code C3h (Kontron OEM IPMB-L Link State) for sensor definition |
| 83 | FRU1 IPMBL State | Discrete | IPMB-L branch from FRU1 fault detection sensor<br>Sensor type = C3h OEM (Kontron OEM IPMB-L link state)<br>Event Reading type code = 6Fh Sensor specific<br>Only offset 2 and 3 are used<br>See OEM table, Sensor type code C3h (Kontron OEM IPMB-L Link State) for sensor definition |
| 84 | FRU2 IPMBL State | Discrete | IPMB-L branch from FRU2 fault detection sensor<br>Sensor type = C3h OEM (Kontron OEM IPMB-L link state)<br>Event Reading type code = 6Fh Sensor specific<br>Only offset 2 and 3 are used<br>See OEM table, Sensor type code C3h (Kontron OEM IPMB-L Link State) for sensor definition |
| 85 | CPU0 Status | Discrete | Processor 0 Status<br>Sensor type = 07h Processor<br>Event Reading type code = 6Fh Sensor Specific<br>Only offset 0,1,5 are used<br>See IPMI v2.0 table 42-3, Sensor type code 07h for sensor definition |

| Sensor ID | Sensor Name | Type | Description |
|---|---|---|---|
| 86 | CPU1 Status | Discrete | Processor 1 Status<br>Sensor type = 07h Processor<br>Event Reading type code = 6Fh Sensor Specific<br>Only offset 0,1,5 are used<br>See IPMI v2.0 table 42-3, Sensor type code 07h for sensor definition |
| 87 | FRU Over Icc | Discrete | FRU Over Current Sensor<br>Sensor type = CBh OEM (Kontron OEM FRU Over Current)<br>Event Reading type code = 03h Digital Discrete offset 0,1 are used,<br>-see OEM table, Sensor type code CBh (Kontron OEM FRU Overcurrent) for sensor definition |
| 88 | FRU Sensor Error | Discrete | FRU Error during external FRU Sensor discovery<br>Sensor type = CCh OEM (Kontron OEM FRU sensor error)<br>Event Reading type code = 03h Digital Discrete offset 0,1 are used,<br>-see OEM table, Sensor type code CCh (Kontron OEM FRU sensor error) for sensor definition |
| 89 | FRU Pwr Denied | Discrete | FRU Power Denial Detection<br>Sensor type = CDh OEM (Kontron FRU Power denied)<br>Event Reading type code = 03h Digital Discrete offset 0,1 are used<br>-see OEM table, Sensor type code CDh (Kontron OEM FRU Power Denied) for sensor definition |
| 90 | FRU MngtPwr Fail | Discrete | FRU Management Power Fail<br>Sensor type = D2h OEM (Kontron FRU Management Power Fail)<br>Event Reading type code = 03h Digital Discrete offset 0,1 are used<br><br>-see OEM table, Sensor type code D2h (Kontron OEM FRU Management Power Fail) for sensor definition |
| 91 | FRU0 Agent | Discrete | FRU Information Agent - FRU0 Data Error Detection<br>Sensor type = C5h OEM (Kontron FRU Info Agent)<br>Event Reading type code = 0Ah Generic Discrete<br>Only offset 6,8 are used<br>See OEM table, Sensor type code C5h (Kontron OEM FRU Information Agent) for sensor definition |

| Sensor ID | Sensor Name | Type | Description |
|---|---|---|---|
| 92 | FRU1 Agent | Discrete | FRU Information Agent - FRU1 Data Error Detection<br>Sensor type = C5h OEM (Kontron FRU Info Agent)<br>Event Reading type code = 0Ah Generic Discrete<br>Only offset 6,8 are used -see OEM table, Sensor type code C5h (Kontron OEM FRU Information Agent) for sensor definition |
| 93 | FRU2 Agent | Discrete | FRU Information Agent - FRU2 Data Error Detection<br>Sensor type = C5h OEM (Kontron FRU Info Agent)<br>Event Reading type code = 0Ah Generic Discrete<br>Only offset 6,8 are used -see OEM table, Sensor type code C5h (Kontron OEM FRU Information Agent) for sensor definition |
| 94 | FRU3 Agent | Discrete | FRU Information Agent - FRU3 Data Error Detection<br>Sensor type = C5h OEM (Kontron FRU Info Agent)<br>Event Reading type code = 0Ah Generic Discrete<br>Only offset 6,8 are used -see OEM table, Sensor type code C5h (Kontron OEM FRU Information Agent) for sensor definition |
| 95 | Ver Change IPMC | Discrete | IPMC Firmware Change Detection<br>Sensor type = 2Bh Version Change<br>Event Reading type code = 6Fh Sensor specific<br>See IPMI v2.0 table 42-3, Sensor type code 2Bh for sensor definition |
| 96 | Ver Change FPGA | Discrete | FPGA Firmware Change Detection<br>Sensor type = 2Bh Version Change<br>Event Reading type code = 6Fh Sensor specific<br>See IPMI v2.0 table 42-3, Sensor type code 2B for sensor definition |
| 97 | Ver Change BIOS | Discrete | BIOS Firmware Change Detection<br>Sensor type = 2Bh Version Change<br>Event Reading type code = 6Fh Sensor specific<br>See IPMI v2.0 table 42-3, Sensor type code 2Bh for sensor definition |
| 98 | EventRcv ComLost | Discrete | Detects communication with the event receiver (ShMc)<br>Sensor type = 1Bh Cable/Interconnect<br>Event Reading type code = 03h Digital Discrete<br>See IPMI v1.5 table 36.2 and table 36.3 for sensor definition |
| 99 | IPMC Reboot | Discrete | IPMC reboot detection<br>Sensor type = 24h Platform Alert<br>Event Reading type code = 03h Digital Discrete<br>Only offset 0,1 are usedà<br>See IPMI v2.0 table 42-3, Sensor type code 24h for sensor definition |

| Sensor ID | Sensor Name | Type | Description |
|---|---|---|---|
| 100 | IPMC Storage Err | Discrete | Management sub-system health: non volatile memory error<br>Sensor type = 28h Management Subsystem Health<br>Event Reading type code = 6Fh Sensor specific<br>Only only offset 1 is used<br>See IPMI v2.0 table 42-3, Sensor type code 28h for sensor definition |
| 101 | IPMC SEL State | Discrete | Specify if the status of the SEL (Cleared/Almost Full/Full)<br>Sensor type = 10h Event Logging Disable<br>Event Reading type code = 6Fh Sensor specific<br>Only offset 2,4,5 are used<br>See IPMI v2.0 table 42-3, Sensor type code 10h (Event Log Disable) for sensor definition |
| 102 | SEL Time Set | Discrete | Specify when SEL time change<br>Sensor type = 12h System Event<br>Event Reading type code = 6Fh Sensor specific<br>Only offset 5 is used<br>See IPMI v2.0 table 42-3, Sensor type code 12h for sensor definition |
| 103 | Jumper Status | Discrete | Reflects on-board jumper presence<br>Sensor type = D3h OEM (Kontron OEM Jumper Status)<br>Event Reading type code = 6Fh Sensor specific, offsets 0 to 14 are used<br>See OEM table, Sensor type code D3h (Kontron OEM Jumper Status) for sensor definition |
| 104 | ME Availability | Discrete | Provides status on the chipset Management Engine<br>Sensor type = 28h Management Subsystem Health<br>Event Reading type code = 0Ah Generic Discrete, offset 2,6,8 are used<br>See IPMI v2.0 table 42-3, event reading type code 0Ah for sensor definition |
| 105 | LAN Base 0 Link | Discrete | Base Interface 0 link status<br>Sensor type = 27h LAN<br>Reading type code = 6Fh Sensor Specific<br>Only offset 0,1 are used<br>See IPMI v2.0 table 42-3, Sensor type code 27h for sensor definition |

| Sensor ID | Sensor Name | Type | Description |
|---|---|---|---|
| 106 | LAN Base 1 Link | Discrete | Base Interface 1 link status<br>Sensor type = 27h LAN<br>Reading type code = 6Fh Sensor Specific<br>Only offset 0,1 are used<br>See IPMI v2.0 table 42-3, Sensor type code 27h for sensor definition |
| 107 | LAN FI 1 Link | Discrete | Fabric Interface 1 link status<br>Sensor type = 27h LAN<br>Reading type code = 6Fh Sensor Specific<br>Only offset 0,1 are used<br>See IPMI v2.0 table 42-3, Sensor type code 27h for sensor definition |
| 108 | LAN FI 2 Link | Discrete | Fabric Interface 2 link status<br>Sensor type = 27h LAN<br>Reading type code = 6Fh Sensor Specific<br>Only offset 0,1 are used<br>See IPMI v2.0 table 42-3, Sensor type code 27h for sensor definition |

| Sensor ID | Sensor Name | Type | Description |
|---|---|---|---|
| 109 | LAN FI 3 Link | Discrete | Fabric Interface 3 link status<br>Sensor type = 27h LAN<br>Reading type code = 6Fh Sensor Specific<br>Only offset 0,1 are used<br>See IPMI v2.0 table 42-3, Sensor type code 27h for sensor definition |
| 110 | LAN FI 4 Link | Discrete | Fabric Interface 4 link status<br>Sensor type = 27h LAN<br>Reading type code = 6Fh Sensor Specific<br>Only offset 0,1 are used<br>See IPMI v2.0 table 42-3, Sensor type code 27h for sensor definition |
| 111 | IPMI Info-1 | Discrete | Internal Management Controller firmware diagnostic<br>Sensor type = C0h Kontron OEM Firmware Info<br>Event Reading type code = 70h Kontron OEM Internal Diagnostic<br>See OEM table, Sensor type code C0h (Kontron OEM Firmware Info) for sensor definition and Event/Reading type code 70h (Kontron OEM Internal Diagnostic) |
| 112 | IPMI Info-2 | Discrete | Internal Management Controller firmware diagnostic<br>Sensor type = C0h Kontron OEM Firmware Info<br>Event Reading type code = 75h Kontron OEM Internal Diagnostic<br>See OEM table, Sensor type code C0h (Kontron OEM Firmware Info) for sensor definition and Event/Reading type code 70h (Kontron OEM Internal Diagnostic) |

### 4.6.2.2 IPMC Health Indicator Sensor Aggregation

The following table shows the sensors involved in the health sensor aggregation.

Table 4-18: IPMC Health Indicator Sensor Aggregation Table

| IPMI sensor ID | Sensor Name |
|---|---|
| 06 | Temp Board Inlet |
| 08 | Temp CPU 0 |
| 09 | Temp CPU 1 |
| 10 | Temp VCORE 0 |
| 11 | Temp VCORE 1 |
| 23 | Brd Input Power |
| 30 | Vcc +12V SUS |
| 31 | Vcc +5V SUS |

| IPMI sensor ID | Sensor Name |
|---|---|
| 32 | Vcc +3.3V SUS |
| 33 | Vcc +1.8V SUS |
| 34 | Vcc +1.5V SUS |
| 35 | Vcc +1.25V SUS |
| 36 | Vcc +1.2V SUS |
| 37 | Vcc +1.0V SUS |
| 38 | Vcc +0.75V SUS |
| 39 | Vcc +1.5V |
| 40 | Vcc +1.2V |
| 41 | Vcc +1.1V ME |
| 42 | Vcc +1.0V A |
| 42 | Vcc VCORE 0 |
| 43 | Vcc VTT CPU 0 |
| 44 | Vcc VDDQ CPU 0 |
| 45 | Vcc VSA CPU 0 |
| 46 | Vcc PLL CPU 0 |
| 47 | Vcc VCORE 1 |
| 48 | Vcc VTT CPU 1 |
| 49 | Vcc VDDQ CPU 1 |
| 50 | Vcc VSA CPU 1 |
| 51 | Vcc PLL CPU 1 |
| 52 | Fuse-Pres A Feed |
| 53 | Fuse-Pres B Feed |
| 55 | Power Good |
| 56 | Power Good Event |
| 57 | IPMI Watchdog |
| 77 | Bios Flash 0 |
| 78 | Bios Flash 1 |

### 4.6.3 FRU Information

Table 4-19:Board Information Area

| Board Information Area | |
|---|---|
| Board Mfg Date | Mon Jan 23 11:14:00 2012 |
| Board Mfg | Kontron |
| Board Product | AT8070 |
| Board Serial | 0123456789 |
| Manufacturing Date / Time | Program to mfg. date |
| Board Part Number | T5009YYY_X-ZZZZZ |

| Board Information Area | |
|---|---|
| Board Manufacturer | Kontron |
| Board FRU ID | FRU5009-12 |
| Board Extra | BI1MAC=XX:XX:XX:XX:XX:XX |
| Board Extra | BI2MAC=XX:XX:XX:XX:XX:XX |
| Board Extra | CPUID=Á |

Table 4-20:Product Information Area

| Product Information Area | |
|---|---|
| Product Manufacturer | Kontron |
| Product Name | AT8070 |
| Product Part Number | T5009YYY_X-ZZZZZ |
| Product Version | X |
| Product Serial | 0123456789 |
| Product FRU ID | FRU5009-12 |

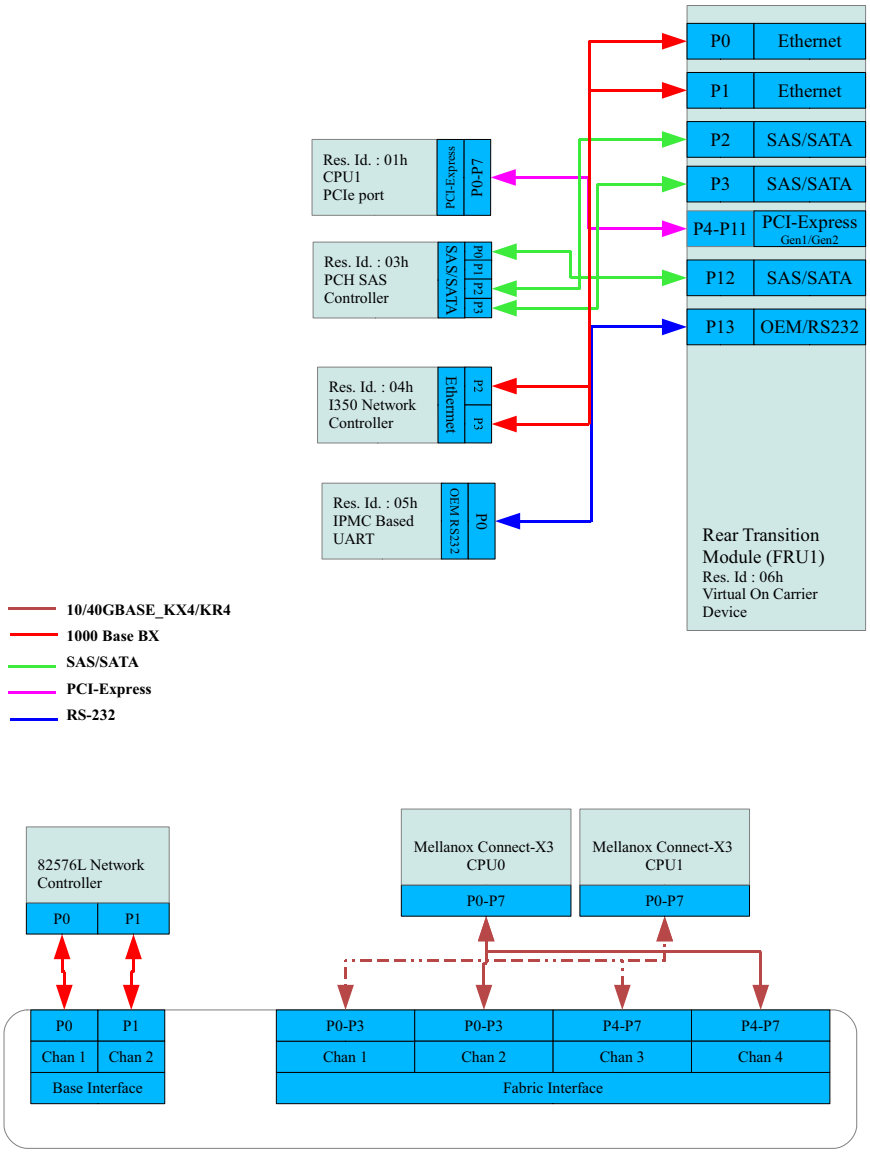
* Variable X, may change on revisions.

### 4.6.3.1 E-Keying Section

The board e-keying information contains PICMG 3.0 R3.0 defined channel and link descriptors required for compatibility computation by the ShMC.

The following figure gives all E-Keying possibilities.

Figure 4-1:E-Keying possibilities.



*Chapter 5*

# Software Setup

5.1 AMI UEFI Setup Program ..... 63
5.2 Boot Utilities ..... 105
5.3 Console Redirection (VT100 Mode) ..... 105

# 5. Software Setup

## 5.1 AMI UEFI Setup Program

All relevant information for operating the board and connected peripherals is stored in the main BIOS section of the SPI.

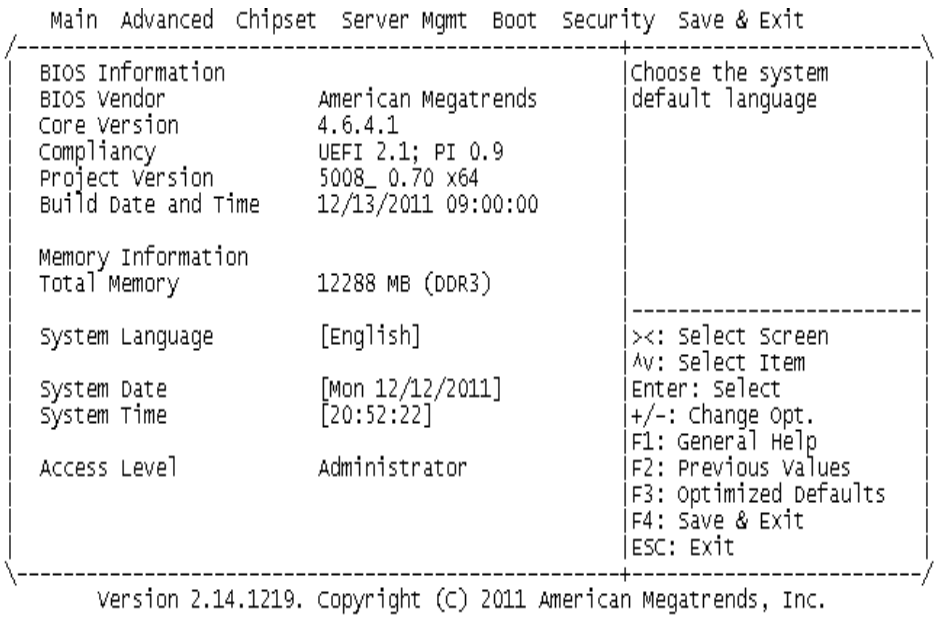
### 5.1.1 Accessing the UEFI Setup Utility

The Unified Extensible Firmware Interface (hereafter known as UEFI) provides an interface between the operating system and the hardware of the AT8070. It uses the AMI Setup program, a setup utility in flash memory that is accessed by pressing the <F2> key at the appropriate time during board boot. This utility is used to set configuration data in the SPI.

To run the AMI Setup program incorporated in the SPI:

- Turn on or reboot the board.
- When you get the following messages, hit <F2> key to enter SETUP.

The main menu of the AMI Aptio Setup Utility appears on the screen.




Setup Default values provide optimum performance settings for all devices and system features.

**Note:**
The setup options described in this section are based on BIOS Version 1.00. The options and default settings may change in a new BIOS release.

**CAUTION**
These parameters have been provided to give control over the board. However, the values for these options should be changed only if the user has a full understanding of the timing relationships involved.

**Note:**
All options in Bold are the default settings.

**WARNING**
While using default 80x25 display mode (default mode), help description box may contain cropped message.

## 5.1.2 Menu Bar

The Menu Bar at the top of the window lists these selections:

| Menu Selection | Description |
|---|---|
| Main | Use this menu for basic board configuration. |
| Advanced | Use this menu to set the Advanced Features available on your board. |
| Security | Use this menu to configure Security features. |
| Boot | Use this menu to determine the booting device order. |
| Server Management | Use this menu to set and view the System Management on your board. |
| Exit | Use this menu to choose Exit option. |

Use the left and right arrows keys to make a selection.

### *5.1.2.1 Legend Bar*

Use the keys listed in the legend bar on the bottom to make your selections or exit the current menu. The chart on the following page describes the legend keys and their alternates.

| Key | Function |
|---|---|
| <F1> | General Help windows. |
| <Esc> | Exit this menu. |
| --> arrow keys | Select a different menu. |
| <Home> or <End> | Move cursor to top or bottom of menu. |
| <PgUp> or <PgDn> | Move cursor to top or bottom of menu. |
| <-> | Select the Previous Value for the field. |
| <+> | Select the Next Value for the field. |

| Key | Function |
|---|---|
| <F2> | Discard the changes for all menus. |
| <F3> | Load the Optimal Default Configuration values for all menus. |
| <F4> | Save and exit. |
| <Enter> | Execute Command, display possible values for this field or Select the sub-menu. |

To select an item, use the arrow keys to move the cursor to the desired parameter. The plus (+) and minus (-) keys will cycle through the options for that field. To reload all default settings, save and/or exit Setup, use the Exit Menu.

To display a submenu, use the arrow keys to move the cursor to the desired submenu and press <Enter>.

### 5.1.2.2 Context-specific Help Window

The help window on the right side of each menu displays the help text for the currently highlighted parameter.

It updates as the selection is moved to a new parameter.

### 5.1.2.3 General Help Windows

Pressing <F1>on any menu brings up the General Help window that describes the legend keys and their alternates:

```
^v><       : Move
Enter      : Select
+/-        : Value
ESC        : Exit
F1         : General Help
F2         : Previous Values
F3         : Optimized Defaults
F4         : Save & Exit Setup

          [OK]
```

Note: The " ^v> <" represent the arrows up, down left, right

## 5.1.3 Main Menu

| Parameter | Options | Description | Help text |
|---|---|---|---|
| BIOS Information | | | |
| BIOS Vendor | | | |
| Core Version | | | |
| Compliancy | | | |
| Project Version | | | |
| Build Date and Time | | | |
| Memory Information | | | |
| Total Memory | | | Total Memory in the System. |
| System Language | | | Choose the system default language |
| System Date | | | Set the Date. Use Tab to switch between Data elements. |
| System Time | | | Set the Time. Use Tab to switch between Time elements. |
| Access Level | | | |

## 5.1.4 Advanced Menu

| Feature | Option | Description | Help text |
|---|---|---|---|
| Spread Spectrum Configuration | | Title | |
| Spread Spectrum Clocking Mode | Disabled, Enabled | | Allows BIOS to Set Clock Spread Spectrum for EMI Control. |
| | | | |
| PCI Subsystem Settings | | Selects sub-menu. | PCI, PCI-X and PCI Express Settings. |
| ACPI Settings | | Selects sub-menu. | System ACPI Parameters. |
| Trusted Computing | | Selects sub-menu. | Trusted Computing Settings |
| WHEA Configuration | | Selects sub-menu. | General WHEA Configuration settings. |
| CPU Configuration | | Selects sub-menu. | CPU Configuration Parameters |
| Runtime Error Logging | | Selects sub-menu. | Runtime Error Logging Support Setup Options |
| Legacy Expansion ROM Configuration | | Selects sub-menu. | Control execution of legacy Expansion ROMs. |
| SATA Configuration | | Selects sub-menu. | SATA Devices Configuration. |
| SAS Configuration | | Selects sub-menu. | SAS Devices Configuration. |
| Thermal Configuration | | Selects sub-menu. | Thermal Configuration |
| USB Configuration | | Selects sub-menu. | USB Configuration Parameters |
| COM Port Configuration | | Selects sub-menu. | COM Port Parameters. |
| Serial Port Console Redirection | | Selects sub-menu. | Serial Port Console Redirection |

### 5.1.4.1 PCI Subsystem Settings sub-menu

| Feature | Option | Description | Help text |
|---|---|---|---|
| PCI Option ROM Handling | | Title | |
| PCI ROM Priority | Legacy ROM, EFI Compatible ROM | | In case of multiple Option ROMs (Legacy and EFI Compatible), specifies what PCI Option ROM to launch. |
| PCI 64bit Resources Handling | | Title | |
| Above 4G Decoding | Disabled, Enabled | | Enables or Disables 64bit capable Devices to be Decoded in Above 4G Address Space (Only if System Supports 64 bit PCI Decoding). |
| PCI Common Settings | | Title | |
| PCI Latency Timer | 32 PCI Bus Clocks, 64 PCI Bus Clocks, 96 PCI Bus Clocks, 128 PCI Bus Clocks, 160 PCI Bus Clocks, 192 PCI Bus Clocks, 224 PCI Bus Clocks, 248 PCI Bus Clocks | | Value to be programmed into PCI Latency Timer Register |
| VGA Palette Snoop | Disabled, Enabled | | Enables or Disables VGA Palette Registers Snooping. |
| PERR# Generation | Disabled, Enabled | | Enables or Disables PCI Device to Generate PERR#. |
| SERR# Generation | Disabled, Enabled | | Enables or Disables PCI Device to Generate SERR#. |
| PCI Express Settings | | Selects sub-menu. | Change PCI Express Devices Settings. |
| PCI Express GEN 2 Settings | | Selects sub-menu. | Change PCI Express GEN Devices Settings. |

#### 5.1.4.1.1 PCI Express Settings sub-menu

| Feature | Option | Description | Help text |
|---|---|---|---|
| PCI Express Device Register Settings | | Title | |
| Relaxed Ordering | Disabled, Enabled | | Enables or Disables PCI Express Device Relaxed Ordering. |
| Extended Tag | Disabled, Enabled | | If ENABLED allows Device to use 8-bit Tag field as a requester. |
| No Snoop | Disabled, Enabled | | Enables or Disables PCI Express Device No Snoop option. |
| Maximum Payload | Auto, 128 Bytes, 256 Bytes, 512 Bytes, 1024 Bytes, 2048 Bytes, 4096 Bytes | | Set Maximum Payload of PCI Express Device or allow System BIOS to select the value. |
| Maximum Read Request | Auto, 128 Bytes, 256 Bytes, 512 Bytes, 1024 Bytes, 2048 Bytes, 4096 Bytes | | Set Maximum Read Request Size of PCI Express Device or allow System BIOS to select the value. |

| Feature | Option | Description | Help text |
|---|---|---|---|
| PCI Express Link Register Settings | | Title | |
| ASPM Support | Disabled, Auto, Force L0s | | Set the ASPM Level: Force L0s - Force all links to L0s State : AUTO - BIOS auto configure : DISABLE - Disables ASPM<br>WARNING: Enabling ASPM may cause some PCI-E devices to fail |
| Extended Synch | Disabled, Enabled | | If ENABLED allows generation of Extended Synchronization patterns. |
| Link Training Retry | Disabled, 2, 3, 5 | | Defines number of Retry Attempts software will take to retrain the link if previous training attempt was unsuccessful. |
| Link Training Timeout (uS) | | | Defines number of Microseconds software will wait before polling 'Link Training' bit in Link Status register. Value range from 10 to 1000 uS. |
| Unpopulated Links | Keep Link ON, Disable Link | | In order to save power, software will disable unpopulated PCI Express links, if this option set to 'Disable Link'. |

#### 5.1.4.1.2 PCI Express GEN 2 Settings sub-menu

| Feature | Option | Description | Help text |
|---|---|---|---|
| PCI Express GEN2 Device Register Settings | | Title | |
| Completion Timeout | Default, Shorter, Longer, Disabled | | In device Functions that support Completion Timeout programmability, allows system software to modify the Completion Timeout value. 'Default' 50us to 50ms. If 'Shorter' is selected, software will use shorter timeout ranges supported by hardware. If 'Longer' is selected, software will use longer timeout ranges. |
| ARI Forwarding | Disabled, Enabled | | If supported by hardware and set to 'Enabled', the Downstream Port disables its traditional Device Number field being 0 enforcement when turning a Type1 Configuration Request into a Type0 Configuration Request, permitting access to Extended Functions in an ARI Device immediately below the Port. Default value: Disabled |
| AtomicOp Requester Enable | Disabled, Enabled | | If supported by hardware and set to 'Enabled', this function initiates AtomicOp Requests only if Bus Master Enable bit is in the Command Register Set. |
| AtomicOp Egress Blocking | Disabled, Enabled | | If supported by hardware and set to 'Enabled', outbound AtomicOp Requests via Egress Ports will be blocked. |
| IDO Request Enable | Disabled, Enabled | | If supported by hardware and set to 'Enabled', this permits setting the number of ID-Based Ordering (IDO) bit (Attribute[2]) requests to be initiated. |

| Feature | Option | Description | Help text |
|---|---|---|---|
| IDO Completion Enable | Disabled, Enabled | | If supported by hardware and set to 'Enabled', this permits setting the number of ID-Based Ordering (IDO) bit (Attribute[2]) requests to be initiated. |
| LTR Mechanism Enable | Disabled, Enabled | | If supported by hardware and set to 'Enabled', this enables the Latency Tolerance Reporting (LTR) Mechanism. |
| End-End TLP Prefix Blocking | Disabled, Enabled | | If supported by hardware and set to 'Enabled', this function will block forwarding of TLPs containing End-End TLP Prefixes. |
| PCI Express GEN2 Link Register Settings | | Title | |
| Target Link Speed | Auto, Force to 2.5 GT/s, Force to 5.0 GT/s | | If supported by hardware and set to 'Force to 2.5 GT/s' for Downstream Ports, this sets an upper limit on Link operational speed by restricting the values advertised by the Upstream component in its training sequences. When 'Auto' is selected HW initialized data will be used. |

| Feature | Option | Description | Help text |
|---|---|---|---|
| Clock Power Management | Disabled, Enabled | | If supported by hardware and set to 'Enabled', the device is permitted to use CLKREQ# signal for power management of Link clock in accordance to protocol defined in appropriate form factor specification. |
| Compliance SOS | Disabled, Enabled | | If supported by hardware and set to 'Enabled', this will force LTSSM to send SKP Ordered Sets between sequences when sending Compliance Pattern or Modified Compliance Pattern. |
| Hardware Autonomous Width | Enabled, Disabled | | If supported by hardware and set to 'Disabled', this will disable the hardware's ability to change link width except width size reduction for the purpose of correcting unstable link operation. |
| Hardware Autonomous Speed | Enabled, Disabled | | If supported by hardware and set to 'Disabled', this will disable the hardware's ability to change link speed except speed rate reduction for the purpose of correcting unstable link operation. |

### 5.1.4.2 CPU Configuration sub-menu

| Feature | Option | Description | Help text |
|---|---|---|---|
| CPU Configuration | | Subtitle | |
| Socket 0 CPU Information | | Selects sub-menu. | Socket specific CPU Information |
| Socket 1 CPU Information | | Selects sub-menu. | Socket specific CPU Information |
| CPU Speed | | Display only | Displays the CPU Speed |
| 64-bit | | Display only | Displays if 64-bit supported |
| Hyper-threading | Disabled, Enabled | | Enabled for Windows XP and Linux (OS optimized for Hyper-Threading Technology) and Disabled for other OS (OS not optimized for Hyper-Threading Technology). When Disabled only one thread per enabled core is enabled. |
| Active Processor Cores | All, 1, 2, 4, 6 | | Number of cores to enable in each processor package. |
| Limit CPUID Maximum | Disabled, Enabled | | Disabled for Windows XP |
| Execute Disable Bit | Disabled, Enabled | | XD can prevent certain classes of malicious buffer overflow attacks when combined with a supporting OS (Windows Server 2003 SP1, Windows XP SP2, SuSE Linux 9.2, RedHat Enterprise 3 Update 3.) |
| Hardware Prefetcher | Disabled, Enabled | | Enable the Mid Level Cache (L2) streamer prefetcher. |
| Adjacent Cache Line Prefetch | Disabled, Enabled | | Enable the Mid Level Cache (L2) prefetching of adjacent cache lines. |

| Feature | Option | Description | Help text |
|---|---|---|---|
| DCU Streamer Prefetcher | Disabled, Enabled | | Enable prefetch of next L1 Data line based upon multiple loads in same cache line. |
| DCU IP Prefetcher | Disabled, Enabled | | Enable prefetch of next L1 line based upon sequential load history. |
| Intel Virtualization Technology | Disabled, Enabled | | When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology |
| CPU Power Management Configuration | | Selects sub-menu. | CPU Power Management Configuration Parameters |

#### 5.1.4.2.1 Socket 0 CPU Information sub-menu

| Feature | Option | Description | Help text |
|---|---|---|---|
| Socket 0 CPU Information | | Subtitle | |
| CPU Signature | | Display only | Displays CPU Signature |
| Microcode Patch | | Display only | CPU Microcode Patch Revision |
| Max CPU Speed | | Display only | Displays the Max CPU Speed |
| Min CPU Speed | | Display only | Displays the Max CPU Speed |
| Processor Cores | | Display only | Displays number of cores. |
| Intel HT Technology | | Display only | When Hyper-threading is enabled, 2 logical CPUS per core is present. |
| Intel VT-x Technology | | Display only | CPU VMX hardware support for virtual machines. |
| L1 Data Cache | | Display only | L1 Data Cache Size |
| L1 Code Cache | | Display only | L1 Code Cache Size |
| L2 Cache | | Display only | L2 Cache Size |
| L3 Cache | | Display only | L3 Cache Size |

#### 5.1.4.2.2 Socket 1 CPU Information sub-menu

| Feature | Option | Description | Help text |
|---|---|---|---|
| Socket 1 CPU Information | | Subtitle | |
| CPU Signature | | Display only | Displays CPU Signature |
| Microcode Patch | | Display only | CPU Microcode Patch Revision |
| Max CPU Speed | | Display only | Displays the Max CPU Speed |
| Min CPU Speed | | Display only | Displays the Max CPU Speed |
| Processor Cores | | Display only | Displays number of cores. |
| Intel HT Technology | | Display only | When Hyper-threading is enabled, 2 logical CPUS per core is present. |
| Intel VT-x Technology | | Display only | CPU VMX hardware support for virtual machines. |
| L1 Data Cache | | Display only | L1 Data Cache Size |
| L1 Code Cache | | Display only | L1 Code Cache Size |
| L2 Cache | | Display only | L2 Cache Size |
| L3 Cache | | Display only | L3 Cache Size |

### 5.1.4.3 Runtime Error Logging sub-menu

| Feature | Option | Description | Help text |
|---|---|---|---|
| Runtime Error Logging Support | Disabled, Enabled | | Enable/Disable Runtime Error Logging Support. |
| Uncorrectable Processor error Log Support | Disabled, Enabled | | Support for Uncorrectable Processor Core and Uncore (Memory, QPI etc) Error Signaling / Logging. |
| CorrectableMemory Error Log Support | Disabled, Enabled | | Support for Correctable Memory Error Signaling / Logging |
| Memory Corr. Error Threshold | | Numeric | Enter the Memory Correctable Error Threshold value |
| PCI Error Logging Support | Disabled, Enabled | | Enable/Disable PCI Error Logging |
| Poison Support | Disabled, Enabled | | Enable/Disable Poison Support. When poisoning is enabled, CPU does not signal the uncorrectable error via MCERR but may signal CMCI if CMCI is enabled |
| Poison Support in IOH | Disabled, Enabled | | Enable/Disable IOH Poison Support. When Poison is enabled, no signaling or logging is done at IIO. Logging and signaling is responsibilty of the Data consumer. |

### 5.1.4.4 Legacy Expansion ROM Configuration sub-menu

| Feature | Option | Description | Help text |
|---|---|---|---|
| BI : GE OpROM, Port 1 | Disabled, Enabled | | Enabled: initializes BI GbE port 1 Expansion ROM.<br>Disabled: PCI Expansion ROM not used to boot the system. |
| BI : GE OpROM, Port 2 | Disabled, Enabled | | Enabled: initializes BI GbE port 2 Expansion ROM.<br>Disabled: PCI Expansion ROM not used to boot the system. |
| FP : GE OpROM, Port 1 | Disabled, Enabled | | Enabled: initializes Front Panel Management GbE port 1 Expansion ROM.<br>Disabled: PCI Expansion ROM not used to boot the system. |
| FP : GE OpROM, Port 2 | Disabled, Enabled | | Enabled: initializes Front Panel Management GbE port 2 Expansion ROM.<br>Disabled: PCI Expansion ROM not used to boot the system. |
| RTM: GE OpROM, Port 1 | Disabled, Enabled | | Enabled: initializes RTM Management GbE port 1 Expansion ROM.<br>Disabled: PCI Expansion ROM not used to boot the system. |
| RTM: GE OpROM, Port 2 | Disabled, Enabled | | Enabled: initializes RTM Management GbE port 2 Expansion ROM.<br>Disabled: PCI Expansion ROM not used to boot the system. |
| RTM Slot OpROM(s) | Disabled, Enabled | | Enabled: initializes all RTM Slot Expansion ROMs.<br>Disabled: no PCI Slot expansion ROM used to boot the system. |

### 5.1.4.5 SAS Configuration sub-menu

| Feature | Option | Description | Help text |
|---|---|---|---|
| SAS Configuration | | Subtitle | |
| SAS Port 0 | | Display only | Displays SAS Device Names if Present |
| SAS Port 1 | | Display only | Displays SAS Device Names if Present |
| SAS Port 2 | | Display only | Displays SAS Device Names if Present |
| SAS Port 3 | | Display only | Displays SAS Device Names if Present |

### 5.1.4.6 Thermal Configuration sub-menu

| Feature | Option | Description | Help text |
|---|---|---|---|
| Thermal Configuration | | Subtitle | |
| Thermal Management | Disabled, Enabled | | Thermal Management Enable/Disable. If Enabled will initilaize the PCH Thermal susbsystem device, D31:F6. |
| ME SMBus Thermal Reporting | Disabled, Enabled | | Enabled/Disabled ME SMBus Thermal Reporting Configuration |
| PCH Temp Read | Disabled, Enabled | | PCH Temperature Read Enable |
| CPU Energy Read | Disabled, Enabled | | CPU Energy Read Enable |
| CPU Temp Read | Disabled, Enabled | | CPU Temperature Read Enable |
| Alert Enable Lock | Disabled, Enabled | | Lock all Alert Enable settings |
| PCH Alert | Disabled, Enabled | | PCH Alert pin enable |
| DIMM Alert | Disabled, Enabled | | DIMM Alert pin enable |

### 5.1.4.7 USB Configuration sub-menu

| Feature | Option | Description | Help text |
|---|---|---|---|
| USB Configuration | | Subtitle | |
| USB Devices: | | Display only | |
| Legacy USB Support | Enabled, Disabled, Auto | | Enables Legacy USB support. AUTO option disables legacy support if no USB devices are connected. DISABLE option will keep USB devices available only for EFI applications. |
| USB Mass Storage Driver | Disabled, Enabled | | Enable/Disable USB Mass Storage Driver Support. |
| EHCI Hand-off | Disabled, Enabled | | This is a workaround for OSes without EHCI hand-off support. The EHCI ownership change should be claimed by EHCI driver. |
| Port 60/64 Emulation | Disabled, Enabled | | Enables I/O port 60h/ 64h emulation support. This should be enabled for the complete USB keyboard legacy support for non-USB aware OSes. |
| USB hardware delays and time-outs: | | Subtitle | |
| USB transfer time-out | 1 sec, 5 sec, 10 sec, 20 sec | | The time-out value for Control, Bulk, and Interrupt transfers. |
| Device reset time-out | 10 sec, 20 sec, 30 sec, 40 sec | | USB mass storage device Start Unit command time-out. |

| Feature | Option | Description | Help text |
|---|---|---|---|
| Device power-up delay | Auto, Manual | | Maximum time the device will take before it properly reports itself to the Host Controller. 'Auto' uses default value: for a Root port it is 100 ms, for a Hub port the delay is taken from Hub descriptor. |
| Device power-up delay in seconds | | Numeric | Delay range is 1..40 seconds, in one second increments |
| Mass Storage Devices: | | Display only | |
| USB Device X | Auto, Floppy, Forced FDD, Hard Disk, CD-ROM | Available on detected device | Mass storage device emulation type. 'AUTO' enumerates devices according to their media format. Optical drives are emulated as 'CDROM', drives with no media will be emulated according to a drive type. |

### 5.1.4.8 COM Port Configuration sub-menu

| Feature | Option | Description | Help text |
|---|---|---|---|
| COM Port Configuration | | Subtitle | |
| COM Port Chip | | Display only | COM Port Parameters. |
| COM Port 1 Configuration | | Selects sub-menu. | Set Parameters of COM port 1 |
| COM Port 2 Configuration | | Selects sub-menu. | Set Parameters of COM port 2 |

#### 5.1.4.8.1 COM Port 1 Configuration sub-menu

| Feature | Option | Description | Help text |
|---|---|---|---|
| COM Port 1 Configuration | | Subtitle | |
| Serial Port | Disabled, Enabled | | Enable or Disable Serial Port (COM) |
| Device Settings | | Display only | Enable or Disable Serial Port (COM) |
| Change Settings | Auto, IO=3F8h; IRQ=4;, IO=3F8h; IRQ=3,4,5,6,7,10,11,12;, IO=2F8h; IRQ=3,4,5,6,7,10,11,12;, IO=3E8h; IRQ=3,4,5,6,7,10,11,12;, IO=2E8h; IRQ=3,4,5,6,7,10,11,12; | | Select an optimal setting for IO device. |

#### 5.1.4.8.2 COM Port 2 Configuration sub-menu

| Feature | Option | Description | Help text |
|---|---|---|---|
| COM Port 2 Configuration | | Subtitle | |
| Serial Port | Disabled, Enabled | | Enable or Disable Serial Port (COM) |
| Device Settings | | Display only | Enable or Disable Serial Port (COM) |
| Change Settings | Auto, IO=2F8h; IRQ=3;, IO=3F8h; IRQ=3,4,5,6,7,10,11,12;, IO=2F8h; IRQ=3,4,5,6,7,10,11,12;, IO=3E8h; IRQ=3,4,5,6,7,10,11,12;, IO=2E8h; IRQ=3,4,5,6,7,10,11,12; | | Select an optimal setting for IO device. |

### 5.1.4.9 Serial Port Console Redirection sub-menu

| Feature | Option | Description | Help text |
|---|---|---|---|
| COM1 | | Subtitle | |
| Console Redirection | Disabled, Enabled | | Console Redirection Enable or Disable. |
| Console Redirection Settings | | Selects sub-menu. | The settings specify how the host computer and the remote computer (which the user is using) will exchange data. Both computers should have the same or compatible settings. |
| COM2 | | Subtitle | |
| Console Redirection | Disabled, Enabled | | Console Redirection Enable or Disable. |
| Console Redirection Settings | | Selects sub-menu. | The settings specify how the host computer and the remote computer (which the user is using) will exchange data. Both computers should have the same or compatible settings. |
| Serial Port for Out-of-Band Management/ | | Subtitle | |
| Windows Emergency Management Services (EMS) | | Subtitle | |
| Console Redirection | Disabled, Enabled | | Console Redirection Enable or Disable. |
| Console Redirection Settings | | Selects sub-menu. | The settings specify how the host computer and the remote computer (which the user is using) will exchange data. Both computers should have the same or compatible settings. |

#### 5.1.4.9.1 Console Redirection Settings sub-menu

| Feature | Option | Description | Help text |
|---|---|---|---|
| Out-of-Band Mgmt Port | COM1, COM2 | | Microsoft Windows Emergency Management Services (EMS) allows for remote management of a Windows Server OS through a serial port. |
| Terminal Type | VT100, VT100+, VT-UTF8, ANSI | | VT-UTF8 is the preferred terminal type for out-of-band management. The next best choice is VT100+ and then VT100. See above, in Console Redirection Settings page, for more Help with Terminal Type/ Emulation. |
| Bits per second | 9600, 19200, 57600, 115200 | | Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds. |

| Feature | Option | Description | Help text |
|---|---|---|---|
| Flow Control | None, Hardware RTS/CTS, Software Xon/Xoff | | Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals. |
| Data Bits | | Display only | Data Bits |
| Parity | | Display only | A parity bit can be sent with the data bits to detect some transmission errors. Even: parity bit is 0 if the num of 1's in the data bits is even. Odd: parity bit is 0 if num of 1's in the data bits is odd. Mark: parity bit is always 1. Space: Parity bit is always 0. Mark and Space Parity do not allow for error detection. They can be used as an additional data bit. |
| Stop Bits | | Display only | Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit. |

### 5.1.4.9.2 COM 0 sub-menu

| Feature | Option | Description | Help text |
|---|---|---|---|
| COM1 | | Subtitle | |
| Console Redirection Settings | | Subtitle | |
| Terminal Type | VT100, VT100+, VT-UTF8, ANSI | | Emulation: ANSI: Extended ASCII char set. VT100: ASCII char set. VT100+: Extends VT100 to support color, function keys, etc. VT-UTF8: Uses UTF8 encoding to map Unicode chars onto 1 or more bytes. |
| Bits per second | 9600, 19200, 38400, 57600, 115200 | | Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds. |
| Data Bits | 7, 8 | | Data Bits |
| Parity | None, Even, Odd, Mark, Space | | A parity bit can be sent with the data bits to detect some transmission errors. Even: parity bit is 0 if the num of 1's in the data bits is even. Odd: parity bit is 0 if num of 1's in the data bits is odd. Mark: parity bit is always 1. Space: Parity bit is always 0. Mark and Space Parity do not allow for error detection. They can be used as an additional data bit. |
| Stop Bits | 1, 2 | | Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit. |

| Feature | Option | Description | Help text |
|---|---|---|---|
| Flow Control | None, Hardware RTS/CTS | | Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals. |
| VT-UTF8 Combo Key Support | Disabled, Enabled | | Enable VT-UTF8 Combination Key Support for ANSI/VT100 terminals |
| Recorder Mode | Disabled, Enabled | | On this mode enabled only text will be send. This is to capture Terminal data. |
| Resolution 100x31 | Disabled, Enabled | | Enables or disables extended terminal resolution |
| Legacy OS Redirection Resolution | 80x24, 80x25 | | On Legacy OS, the Number of Rows and Columns supported redirection |
| Putty KeyPad | VT100, LINUX, XTERMR6, SCO, ESCN, VT400 | | Select FunctionKey and KeyPad on Putty. |
| Install Legacy OS through Remote | Disabled, Enabled | | Enable to Install Legacy OS like Linux in text/ graphics mode through redirection When System has Vga. This might not work for all Linux Versions. |
| Redirection After BIOS POST | Always Enable, BootLoader | | The Settings specify if BootLoader is selected than Legacy console redirection is disabled before booting to Legacy OS. Default value is Always Enable which means Legaacy console Redirection is enabled for Legacy OS. |

### 5.1.4.9.3 COM 2 sub-menu

| Feature | Option | Description | Help text |
|---|---|---|---|
| COM2 | | Subtitle | |
| Console Redirection Settings | | Subtitle | |
| Terminal Type | VT100, VT100+, VT-UTF8, ANSI | | Emulation: ANSI: Extended ASCII char set. VT100: ASCII char set. VT100+: Extends VT100 to support color, function keys, etc. VT-UTF8: Uses UTF8 encoding to map Unicode chars onto 1 or more bytes. |
| Bits per second | 9600, 19200, 38400, 57600, 115200 | | Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds. |
| Data Bits | 7, 8 | | Data Bits |
| Parity | None, Even, Odd, Mark, Space | | A parity bit can be sent with the data bits to detect some transmission errors. Even: parity bit is 0 if the num of 1's in the data bits is even. Odd: parity bit is 0 if num of 1's in the data bits is odd. Mark: parity bit is always 1. Space: Parity bit is always 0. Mark and Space Parity do not allow for error detection. They can be used as an additional data bit. |
| Stop Bits | 1, 2 | | Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit. |

| Feature | Option | Description | Help text |
|---|---|---|---|
| Flow Control | None, Hardware RTS/CTS | | Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals. |
| VT-UTF8 Combo Key Support | Disabled, Enabled | | Enable VT-UTF8 Combination Key Support for ANSI/VT100 terminals |
| Recorder Mode | Disabled, Enabled | | With this mode enabled only text will be sent. This is to capture Terminal data. |
| Resolution 100x31 | Disabled, Enabled | | Enables or disables extended terminal resolution |
| Legacy OS Redirection Resolution | 80x24, 80x25 | | On Legacy OS, the Number of Rows and Columns supported redirection |

### 5.1.5 Chipset

| Feature | Option | Description | Help text |
|---|---|---|---|
| North Bridge | | Selects sub-menu. | North Bridge Parameters |
| South Bridge | | Selects sub-menu. | South Bridge Parameters |
| ME Subsystem | | Selects sub-menu. | ME Subsystem Parameters |

### 5.1.5.1 North Bridge sub-menu

| Feature | Option | Description | Help text |
|---|---|---|---|
| IOH Configuration | | Selects sub-menu. | IOH Configuration Page |
| QPI Configuration | | Selects sub-menu. | QPI Configuration Page |
| Compatibility RID | Enabled, Disabled | | Support for Compatibility Revision ID (CRID) Functionality mentioned in Sandybridge bios spec |
| Memory Configuration | | Subtitle | |
| Total Memory | | Display only | Total Memory in the System. |
| Current Memory Mode | | Display only | Current Memory Configuration |
| Current Memory Speed | | Display only | DDR3 Memory Operating Speed. |
| Mirroring | | Display only | Possible Memory mode |
| Sparing | | Display only | Possible Memory mode |
| Memory Mode | Independent, Mirroring, Lock Step | | Select the mode for memory initialization. |
| Spare Err Threshold | | Numeric | Set Spare Err Threshold |
| DRAM RAPL BWLIMIT | 0, 1, 8, 16 | | DRAM RAPL BWLIMIT : Intel Recommended values |
| Perfmon and DFX devices | HIDE | HIDE, UNHIDE | Perfmon and DFX devices can be hidden or unhidden |
| DRAM RAPL MODE | Disabled, DRAM RAPL MODE0, DRAM RAPL MODE1 | | DRAM RAPL MODES: Disabled/MODE0/MODE1 |
| Data Integrity Mode | DRAM Non-ECC, DRAM ECC | | ECC: ECC Checking enables. Non-ECC: Use only for testing purposes. |
| Numa | Disabled, Enabled | | Enable or Disable Non uniform Memory Access (NUMA). |
| MPST Support | Disabled, Enabled | | Enable or Disable MPST Support. Along with enabling MPST Support, it also requires NUMA to be enabled and Channel Interleaving to be set to 1-way for MPST tables to be published. |

| Feature | Option | Description | Help text |
|---|---|---|---|
| DDR Speed | Auto, Force DDR3 800, Force DDR3 1066, Force DDR3 1333, Force DDR3 1600, Force DDR3 1866 | | Force DDR Speed |
| Channel Interleaving | Auto, 1 Way, 2 Way, 3 Way, 4 Way | | Select different Channel Interleaving setting. |
| Rank Interleaving | Auto, 1 Way, 2 Way, 4 Way, 8 Way | | Select different rank Interleaving setting. |
| Patrol Scrub | Disabled, Enabled | | Enable/Disable Patrol Scrub |
| Demand Scrub | Disabled, Enabled | | Enable/Disable Demand Scrubing Feature |
| Data Scrambling | Disabled, Enabled | | Enable/Disable Data Scrambling |
| Device Tagging | Disabled, Enabled | | Enable/Disable Device Tagging |
| Rank Margin | Disabled, Enabled | | Enable/Disable Rank Margin |
| Thermal Throttling | Disabled, OLTT, CLTT | | CLTT - Closed Loop Thermal Throttling, OLTT - Open Loop Thermal Throttling |
| OLTT Peak BW % | | Numeric | Valid Offset 25 - 100. This is a percentage of the peak bandwidth allowed for OLTT |
| Altitude | Auto, 300 M, 900 M, 1500 M, 3000 M | | The system altitude above the sea level in meters |
| Serial Message Debug Level | Minimum, Maximum, Trace, Memory Training | | Select Serial Message Debug Level |
| DIMM Information | | Selects sub-menu. | Display DIMM presence and Size information. |

#### 5.1.5.1.1 DIMM Information sub-menu

| Feature | Option | Description | Help text |
|---|---|---|---|
| CPU Socket 0 DIMM Information | | Subtitle | |
| Node 0 Ch 0 Dimm 0 | | Display only | Memory in the Slot. |
| Node 0 Ch 1 Dimm 0 | | Display only | Memory in the Slot. |
| Node 0 Ch 2 Dimm 0 | | Display only | Memory in the Slot. |
| Node 0 Ch 3 Dimm 0 | | Display only | Memory in the Slot. |

| Feature | Option | Description | Help text |
|---|---|---|---|
| CPU Socket 1 DIMM Information | | Subtitle | |
| Node 1 Ch 0 Dimm 0 | | Display only | Memory in the Slot. |
| Node 1 Ch 1 Dimm 0 | | Display only | Memory in the Slot. |
| Node 1 Ch 2 Dimm 0 | | Display only | Memory in the Slot. |
| Node 1 Ch 3 Dimm 0 | | Display only | Memory in the Slot. |

#### 5.1.5.1.2 IOH Configuration sub-menu

| Feature | Option | Description | Help text |
|---|---|---|---|
| Intel(R) VT for Directed I/O Configuration | | Selects sub-menu. | Intel(R) VT for Directed I/O Configuration |
| Intel(R) I/OAT | Disabled, Enabled | | Enables/Disables Intel(R) I/O Acceleration Technology (I/OAT). |
| DCA Support | Disabled, Enabled | | Enables/Disables Direct Cache Access Support. |
| VGA Priority | Onboard, Offboard | | Decides priority between onboard and 1st offboard video device found. |
| TargetVGA | | Display Only | TargetVGA from RootPort under CPU0/CPU1/CPU2/CPU3 |
| Gen3 Equalization WA's | Enabled, Disabled | | Support for Gen3 Equalization Workarounds mentioned in SNB_BSU Version 0.83 |
| Gen3 Equalization Fail WA | Enabled, Disabled | | 3875734: PCIE: on Gen3 Eq fail, InitFC is bypassed at Gen1 |
| Gen3 Equalization Phase 2/3 WA | Enabled, Disabled | | 3875700: PCIe* at 8 GT/s may not Train Correctly |
| Equalization Phase 2/3 Supported | Enabled, Disabled | | Enable/Disable based Equalization Phase(2,3) Supported or Not |
| Gen3 Equalization Redoing WA | Enabled, Disabled | | 3246043: Not sending EQ TS1 in REC_RCVRLOCK when redoing equalization |

| Feature | Option | Description | Help text |
|---|---|---|---|
| IOH Resource Selection Type | Auto, Manual | | Allows to select Auto/ Manual. When Auto option is selected PCI resource allocation across multiple IOHs is optimized automatically based on the PCI devices present. With Manual option user can force the PCI resource allocation across multiple IOHs based on the ratios selected. |
| MMIOH Size | 1G, 2G, 4G, 8G, 16G, 32G, 64G, 128G | | Select number of 1GB contiguous regions to be assigned for MMIOH space per CPU |
| MMCFG BASE | 0x80000000, 0xA0000000, 0xC0000000 | | MMCFG BASE Values |
| Io Ratio Skt0 | | Numeric | Value ranges are from [1-8].Ratio calculated based on : value selected / total value of all sockets. If granularity fails, resources will be allocated equally for all sockets. |
| Io Ratio Skt1 | | Numeric | Value ranges are from [1-8].Ratio calculated based on : value selected / total value of all sockets. If granularity fails, resources will be allocated equally for all sockets. |
| Mmio Ratio Skt0 | | Numeric | Value ranges are from [1-8].Ratio calculated based on : value selected / total value of all sockets with 64MB alignment. |
| Mmio Ratio Skt1 | | Numeric | Value ranges are from [1-8].Ratio calculated based on : value selected / total value of all sockets. If granularity fails, resources will be allocated equally for all sockets. |
| IOH 0 PCIe port | | Subtitle | |
| Feature: PORT 2A (FI Ch2&4) | Disabled, Enabled | | Enable/Disable Data Direct I/O |

| Feature | Option | Description | Help text |
|---|---|---|---|
| IOH 1 PCIe port Speed Control | | Subtitle | |
| RTM Port Link Speed | Auto, GEN1, GEN2, GEN3 | | Select 'Auto' to check for T5705 (RTM8050) and force GEN1 if detected, else GEN2 is used. Select 'GEN1' if Hot-Plug of T5705 is to be done later. |
| IOH 1 PCIe port Data Direct I/O Control | | Subtitle | |
| PORT 1A (RTM) | Disabled, Enabled | | Enable/Disable Data Direct I/O |
| PORT 2A (FI Ch1&3) | Disabled, Enabled | | Enable/Disable Data Direct I/O |
| PORT 2C (BI) | Disabled, Enabled | | Enable/Disable Data Direct I/O |
| PORT 2D (MGMT) | Disabled, Enabled | | Enable/Disable Data Direct I/O |

### 5.1.5.2 QPI Configuration sub-menu

| Feature | Option | Description | Help text |
|---|---|---|---|
| Current QPI Link Speed | | Display Only | Current QPI Link Speed |
| Current QPI Link Freq | | Display Only | Current QPI Link Freq |
| Isoc | Disabled, Enabled | | Enbale /Disable Isoc |
| QPI Link Speed Mode | Slow, Fast | | Select the QPI link speed as either the Fast mode or Slow Mode |
| QPI Link Frequency Select | Auto, 6.4 GT/s, 7.2 GT/s, 8.0 GT/s | | Allows for selecting the QPI Link Frequency |
| QPI Link0s | Disabled, Enabled | | Enable or Disable QPI Link0s |
| QPI Link0p | Disabled, Enabled | | Enable or Disable QPI Link0p |
| QPI Link1 | Disabled, Enabled | | Enable or Disable QPI Link1 |

### 5.1.5.3 South Bridge sub-menu

| Feature | Option | Description | Help text |
|---|---|---|---|
| PCH Information | | Subtitle | |
| Name | | Display only | PCH Name |
| Stepping | | Display only | PCH Stepping |
| SB Chipset Configuration | | Subtitle | |
| PCH Compatibility RID | Disabled, Enabled | | Support for PCH Compatibility Revision ID (CRID) Functionality. |
| SMBus Controller | Disabled, Enabled | | Enabled/Disabled SMBus Controller. |
| SW SMI Timer | Disabled, Auto | | Auto - The SW SMI Timer will be enabled as necessary<br>Disable - Force the SW SMI Timer disabled |
| SLP_S4 Assertion Stretch Enable | Disabled, Enabled | | Enabled/Disabled SLP_S4# Assertion Stretch. |
| SLP_S4 Assertion Width | 1-2 Seconds, 2-3 Seconds, 3-4 Seconds, 4-5 Seconds | | Select a minimum assertion width of the SLP_S4# signal. |
| Deep Sx | Disabled, Enabled in S5(Battery), Enabled in S5, Enabled in S4 and S5(Battery), Enabled in S4 and S5 | | Deep Sx configuration. NOTE:Mobile platforms support Deep S4/S5 in DC only and Desktop platforms support Deep S4/S5 in AC only. |
| Disable SCU devices | Disabled, Enabled | | Enable/Disable Patsburg SCU devices. |
| Onboard SAS Oprom | Disabled, Enabled | | Enabled/Disabled onboard SAS option rom. When Enabled is selected (to access SAS disks on the RTM), Disable SCU devices feature must be set to Disabled. |
| High Precision Event Timer Configuration | | Subtitle | |
| High Precision Timer | Disabled, Enabled | | Enabled/Disabled the High Precision Event Timer. |
| PCI Express Ports Configuration | | Selects sub-menu. | PCI Express Ports Configuration |
| USB Configuration | | Selects sub-menu. | USB Configuration |

#### 5.1.5.3.1 PCI Express Ports Configuration sub-menu

| Feature | Option | Description | Help text |
|---|---|---|---|
| PCI Express Ports Configuration | | Subtitle | |
| PCI Express Port 8 | Disabled, Enabled, Auto | | Enabled/Disabled the PCI Express Ports in the Chipset. |
| PME SCI | Disabled, Enabled | | Enable or disable the PCI Express PME SCI. |
| DMI Vc1 Control | Enabled, Disabled | | Enable/Disable DMI Vc1 |
| DMI Vcp Control | Enabled, Disabled | | Enable/Disable DMI Vcp |
| DMI Vcm Control | Enabled, Disabled | | Enable/Disable DMI Vcm |

#### 5.1.5.3.2 USB Configuration sub-menu

| Feature | Option | Description | Help text |
|---|---|---|---|
| USB Configuration | | Subtitle | |
| EHCI Controller 1 | Disabled, Enabled | | Enabled/Disabled USB 2.0 (EHCI) Support |
| EHCI Controller 2 | Disabled, Enabled | | Enabled/Disabled USB 2.0 (EHCI) Support |
| USB Port 0 (SSD0) | Disabled, Enabled | | Enabled/Disabled USB Port 0 |
| USB Port 2 (FP0) | Disabled, Enabled | | Enabled/Disabled USB Port 2 |
| USB Port 5 (RTM0) | Disabled, Enabled | | Enabled/Disabled USB Port 5 |
| USB Port 6 (RTM1) | Disabled, Enabled | | Enabled/Disabled USB Port 6 |
| USB Port 7 (FP1) | Disabled, Enabled | | Enabled/Disabled USB Port 7 |
| USB Port 11 (MC0) | Disabled, Enabled | | Enabled/Disabled USB Port 11 |
| USB Port 13 (MC1) | Disabled, Enabled | | Enabled/Disabled USB Port 13 |

#### 5.1.5.4 ME Subsystem sub-menu

| Feature | Option | Description | Help text |
|---|---|---|---|
| Intel ME Subsystem Configuration | | Subtitle | |
| ME Subsystem | Disabled, Enabled | | ME Subsystem Help |
| ME BIOS Interface Version | | Display only | ME BIOS Interface Version implemented on ME side |
| ME Version | | Display only | ME firmware Version |
| ME FW Status Value : | | Display only | |
| ME FW State : | | Display only | Current operation state of the FW |
| ME FW Operation State : | | Display only | Operation that Me is currently functioning in. |
| ME FW Error Code : | | Display only | Error value of the FW |
| ME Ext FW Status Value : | | Display only | |
| BIOS Booting Mode : | | Display only | BIOS POST Booting mode |
| Cores Disabled : | | Display only | No. of cores that should be disabled on each CPU Socket |
| ME FW SKU Information : | | Display only | Firmware SKU Information |

## 5.1.6 Server Management

#### 5.1.6.1 Managed FRU Deactivate Policies sub-menu

| Feature | Option | Description | Help text |
|---|---|---|---|
| Managed FRU Deactivate Policies | | Subtitle | |
| On RTM Deactivation | Deactivate FRU0, Deactivate FRU1 | | Select FRU0 to shutdown the whole board or FRU1 to shutdown the RTM only |
| On RTM Disk Deactivation | Deactivate FRU0, Deactivate RTM Disk | | Select FRU0 to shutdown the whole board or RTM Disk to shutdown the RTM Disk only |

### 5.1.6.2 Power Limit options sub-menu

| Feature | Option | Description | Help text |
|---|---|---|---|
| Power Limit options | | Subtitle | |
| Power Limit | Activated, Deactivated | | Activate/Deactivate Power Limit option |
| Power Limit Value | | Numeric | Set the Power Limit threshold value |
| Exception Action | No action, Hard Power Off System and log event to SEL, Log event to SEL only | | Exception action taken if the Power Limit is exceeded and cannot be controlled within the Correction time limit |
| Correction Time Limit | | Numeric | Maximum time in miliseconds taken to limit the power after the platform power has reached the power limit before the Exception Action will be taken |
| Statistics Sampling period | | Numeric | Statistics sampling period in seconds |

### 5.1.6.3 Watchdog Configuration sub-menu

| Feature | Option | Description | Help text |
|---|---|---|---|
| Watchdog Configuration | | Subtitle | |
| FRB-2 Timer | Enabled, Disabled | | Enable or Disable FRB-2 timer(POST timer) |
| FRB-2 Timer timeout | 3 minutes, 4 minutes, 5 minutes, 6 minutes | | Enter value Between 3 to 6 min for FRB-2 Timer Expiration value |
| FRB-2 Timer Policy | Do Nothing, Reset, Power Down, Power Cycle | | Configure how the system should respond if the FRB-2 Timer expires. Not available if FRB-2 Timer is disabled. |
| OS Watchdog Timer | Enabled, Disabled | | If enabled, starts a BIOS timer which can only be shut off by Management Software after the OS loads. Helps determine that the OS successfully loaded or follows the OS Boot Watchdog Timer policy. |
| OS Wtd Timer Timeout | 30 seconds, 1 minute, 3 minutes, 5 minutes, 10 minutes, 15 minutes, 20 minutes | | Configure the length of the OS Boot Watchdog Timer. Not available if OS Boot Watchdog Timer is disabled. |
| OS Wtd Timer Policy | Do Nothing, Reset, Power Down, Power Cycle | | Configure how the system should respond if the OS Boot Watchdog Timer expires. Not available if OS Boot Watchdog Timer is disabled. |

### 5.1.6.4 FRU Information sub-menu

| Feature | Option | Description | Help text |
|---|---|---|---|
| FRU Information | | Subtitle | |
| System Manufacturer | | Display only | System Manufacturer |
| System Product Name | | Display only | System Product Name |
| System Version | | Display only | System Version |
| System Serial Number | | Display only | System Serial Number |
| Board Manufacturer | | Display only | Board Manufacturer |
| Board Product Name | | Display only | Board Product Name |
| Board Version | | Display only | Board Version |
| Board Serial Number | | Display only | Board Serial Number |

### 5.1.6.5 BMC Network configuration sub-menu

| Feature | Option | Description | Help text |
|---|---|---|---|
| BMC network configuration | | Subtitle | |
| Lan channel 1 configuration | | Selects sub-menu. | Lan channel 1 configuration |
| Lan channel 2 configuration | | Selects sub-menu. | Lan channel 2 configuration |

#### 5.1.6.5.1 Lan channel 1 configuration sub-menu

| Feature | Option | Description | Help text |
|---|---|---|---|
| Lan channel 1 configuration | | Subtitle | |
| Configuration source | Disabled, Static, Dynamic | | Select to configure LAN channel parameters statically or dynamically (DHCP). Changes will be applied on next reboot. |
| BMC IP address | | Display only if Dynamic | Enter BMC IP address. |
| Subnet mask | | Display only if Dynamic | Enter subnet mask. |
| Gateway IP address | | Display only if Dynamic | Enter Gateway IP address. |
| BMC IP address | | | Enter BMC IP address. |
| Subnet mask | | | Enter subnet mask. |
| Gateway IP address | | | Enter Gateway IP address. |
| BMC MAC address | | Display only | Enter BMC MAC address. |
| VLAN Tagged Support | | | Select if VLAN Tagged Packets are to be added or not. |
| 802.1q VLAN ID Value | | Numeric | Enter VLAN ID value in decimal. VLAN ID must be between 1 and 4094. |
| 802.1q VLAN Priority | | Numeric | Enter VLAN Priority value in decimal. Proper value below 8. |

### 5.1.6.5.2 Lan channel 2 configuration sub-menu

| Feature | Option | Description | Help text |
|---|---|---|---|
| Lan channel 2 configuration | | Subtitle | |
| Configuration source | Disabled, Static, Dynamic | | Select to configure LAN channel parameters statically or dynamically (DHCP). Changes will be applied on next reboot. |
| BMC IP address | | Display only if Dynamic | Enter BMC IP address. |
| Subnet mask | | Display only if Dynamic | Enter subnet mask. |
| Gateway IP address | | Display only if Dynamic | Enter Gateway IP address. |
| BMC IP address | | | Enter BMC IP address. |
| Subnet mask | | | Enter subnet mask. |
| Gateway IP address | | | Enter Gateway IP address. |
| BMC MAC address | | Display only | Enter BMC MAC address. |
| VLAN Tagged Support | | | Select if VLAN Tagged Packets are to be added or not. |
| 802.1q VLAN ID Value | | Numeric | Enter VLAN ID value in decimal. VLAN ID must be between 1 and 4094. |
| 802.1q VLAN Priority | | Numeric | Enter VLAN Priority value in decimal. Proper value below 8. |

## 5.1.7 Boot

| Feature | Option | Description | Help text |
|---|---|---|---|
| Boot Configuration | | Subtitle | |
| Setup Prompt Timeout | | Numeric | Number of seconds to wait for setup activation key. 65535(0xFFFF) means indefinite waiting. |
| Bootup NumLock State | On, Off | | Select the keyboard NumLock state |
| Quiet Boot | Disabled, Enabled | | Enables or disables Quiet Boot option |
| Retry Boot Sequence | Disabled, Enabled | | Enable this option to Retry the Boot Sequence until a successful boot (infinite retries). |
| CSM16 Module Version | | Display only | CSM16 Module Version |
| GateA20 Active | Upon Request, Always | | UPON REQUEST - GA20 can be disabled using BIOS services. ALWAYS - do not allow disabling GA20; this option is useful when any RT code is executed above 1MB. |
| Option ROM Messages | Force BIOS, Keep Current | | Set display mode for Option ROM |
| INT19 Trap Response | Immediate, Postponed | | BIOS reaction on INT19 trapping by Option ROM:<br>IMMEDIATE - execute the trap right away;<br>POSTPONED - execute the trap during legacy boot. |
| CSM Support | Disabled, Enabled, Auto | | Enable/Disable CSM Support. If Auto is selected, based on OS, CSM will be enabled/ disabled automatically. |
| Boot Option Priorities | | Subtitle | |
| Boot Option X | | | Sets the system boot order |
| Boot Option X+1 | | | |
| Network Device BBS Priorities | | Display only if device are present. | Set the order of the legacy devices in this group |
| X Device BBS Priorities | | Display only if device are present. | Set the order of the legacy devices in this group |

## 5.1.8 Security

| Feature | Option | Description | Help text |
|---|---|---|---|
| Password Description | | Subtitle | |
| If ONLY the Administrator's password is set, then this only limits access to Setup and is only asked for when entering Setup. If ONLY the User's password is set, then this is a power on password and must be entered to boot or enter Setup. In Setup the User will have Administrator rights. The password length must be in the following range: Minimum length 3 Maximum length 20 | | Text | |
| Administrator Password | | | Set Administrator Password |
| User Password | | | Set User Password |

## 5.1.9 Save & Exit

| Feature | Option | Description | Help text |
|---|---|---|---|
| Save Changes and Exit | | | Exit system setup after saving the changes. |
| Discard Changes and Exit | | | Exit system setup without saving any changes. |
| Save Changes and Reset | | | Reset the system after saving the changes. |
| Discard Changes and Reset | | | Reset system setup without saving any changes. |
| Save Options | | Subtitle | |
| Save Changes | | | Save Changes done so far to any of the setup options. |
| Discard Changes | | | Discard Changes done so far to any of the setup options. |
| Restore Defaults | | | Restore/Load Default values for all the setup options. |

| Feature | Option | Description | Help text |
|---|---|---|---|
| Save as User Defaults | | | Save the changes done so far as User Defaults. |
| Restore User Defaults | | | Restore the User Defaults to all the setup options. |
| | | | |
| Boot Override | | Subtitle | |
| Boot Option X | | Select device to boot | |
| Boot Option X+1 | | Select device to boot | |

# 5.2 Boot Utilities

## 5.2.1 Entering UEFI BIOS Setup Menu

Pressing <F2> during POST enters UEFI BIOS Setup.

## 5.2.2 SAS Option ROM (RTM806X)

To access the SAS Option ROM, follow the procedure listed below.

1 The RTM806X (with at least two drives attached) must be present.

2 Option ROM for SAS needs to be enabled in the UEFI BIOS (Setup -> Chipset -> South Bridge -> Onboard SAS Oprom).

3 Press "CTRL-I" during the execution of the option ROM.

The SAS configuration utility menu is now available.

# 5.3 Console Redirection (VT100 Mode)

The VT100 operating mode allows remote setup/operated of the board. This configuration requires a remote terminal that must be connected to the board through a serial communication link.

## 5.3.1 Requirements

The terminal should emulate a VT100 or an ANSI terminal. Terminal emulation programs such as Putty, Telix©, HyperTherminal(Windows), minicom(Linux) or ProComm©(Windows) can also be used.

## 5.3.2 ANSI and VT100 Keystroke Mapping

| | |
|---|---|
| Up | <ESC>[A |
| Down | <ESC>[B |
| Right | <ESC>[C |
| Left | <ESC>[D |
| Home | <ESC>[H |
| End | <ESC>[K |
| F1 | <ESC>OP |
| F2 | <ESC>OQ |
| F3 | <ESC>OR |
| F4 | <ESC>OT |

## 5.3.3 VT-UTF8 Keystroke Mapping

The following "escape sequences" are defined in the "Conventions for Keys Not in VT100 Terminal Definition and ASCII Character Set" section of "Standardizing Out-of-Band Management Console Output and Terminal Emulation (VT-UTF8 and VT100+)",available for download at microsoft.com.

| | |
|---|---|
| F1 Key | <ESC>1 |
| F2 Key | <ESC>2 |
| F3 Key | <ESC>3 |
| F4 Key | <ESC>4 |
| F5 Key | <ESC>5 |
| F6 Key | <ESC>6 |
| F7 Key | <ESC>7 |
| F8 Key | <ESC>8 |
| F9 Key | <ESC>9 |
| F10 Key | <ESC>0 |
| F11 Key | <ESC>! |
| F12 Key | <ESC>@ |
| Alt Modifier | <ESC>^A |
| Control Modifier | <ESC>^C |
| Home Key | <ESC>h |
| End Key | <ESC>k |
| Insert Key | <ESC>+ |
| Delete Key | <ESC>- |
| Page Up Key | <ESC>? |
| Page Down Key | <ESC>/ |

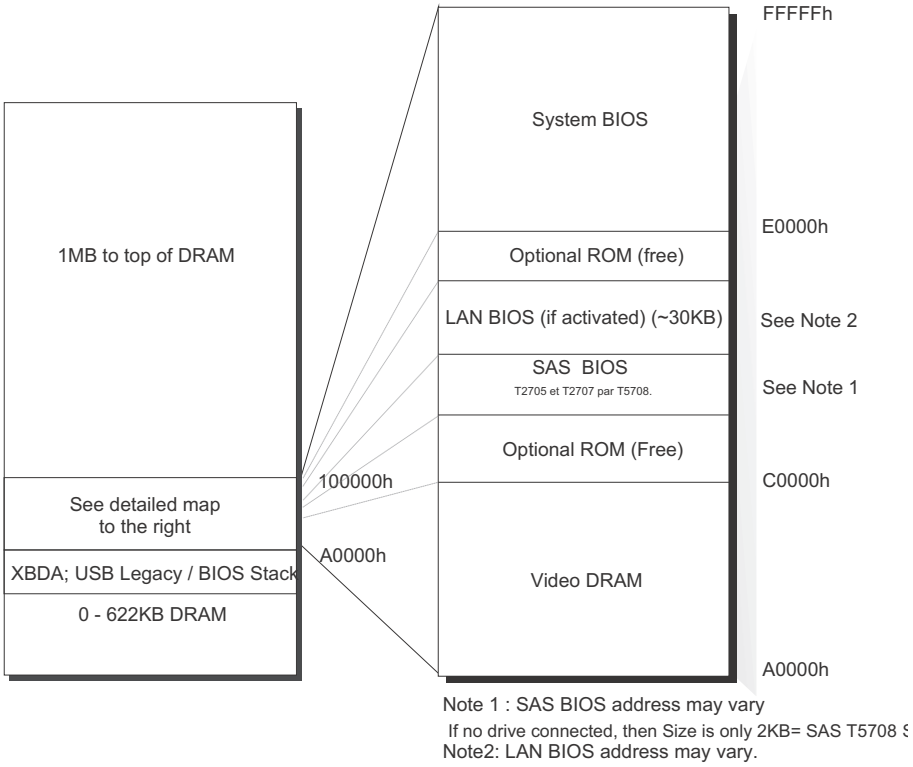
These "escape sequences" are supported by VT-UTF8 compliant terminal connections, such as Windows Server 2003 Emergency Management Services (EMS).

AMI Aptio UEFI Serial Redirection supports these key sequences under two configurations:

- "Terminal Type" setup question is set to "VT-UTF8"
- "Terminal Type" setup question is set to "VT100" or "ANSI" and "VTUTF8 Combo Key Support" setup question is set to "Enabled"

# A. Memory & I/O Maps

## A.1 Memory Mapping




| Address | Function |
|---|---|
| 00000-9B7FF | 0-622 KB DRAM |
| 9B800-9FFFF | 622KB - 640 KB XBDA; USB Legacy / BIOS Stack |
| A0000-BFFFF | Video DRAM |
| C0000-DBFFF | Optional ROM (Free)<br>LAN BIOS around 30KB if activated, address may vary<br>External Fiber Channel BIOS 18KB-64KB , address may vary |
| E0000-FFFFF | System BIOS |
| 100000-PCI Memory | DRAM available |

**Note:**
Actual memory availability to OS depends on the total amount of DRAM installed and the PCI resource usage.

# A.2 Kontron I/O Mapping

| Address | Optional Address | Function |
|---|---|---|
| 000-01F | | DMA Controller 1 |
| 020-03F | | Interrupt Controller 1 |
| 040-05F | | Timer |
| 060-06F | | Keyboard (USB Emulation) |
| 070-07F | | Real-time clock |
| 080-09F | | DMA Page Register |
| 0A0-0BF | | Interrupt Controller 2 |
| 0C0-0DF | | DMA Controller 2 |
| 0F0-0F1, 0F8-0FF | | Math Coprocessor |
| 1F0-1F7, 3F6 | | Primary IDE |
| 170-177, 376 | | Secondary IDE |
| 378-37F | | Parallel Port (Used as PLD POD) |
| 3F8-3FF (COM1) | | Serial Port 1 (COM1 by default) |
| 2F8-2FF (COM2) | | Serial Port 2 (COM2 by default) |
| 400-7FF | | Chipset Reserved |
| 800-9FF | | Chipset Reserved |
| A00-A1F | | Kontron Registers (on-board) |
| CA0-CAF | | BMC public and private KCS interfaces |

# A.3 PCI IDSEL and Device Numbers

| BUS# | DEV# | V. ID | D. ID | Funct. # | Description | PCI Description |
|---|---|---|---|---|---|---|
| 00 | 00 | 8086 | 3c00 | 0 | Host bridge: Intel Corporation Xeon E5/Core i7 DMI2 (rev 06) | IIO #0 |
| 00 | 02 | 8086 | 3c04 | 0 | PCI bridge: Intel Corporation Xeon E5/Core i7 IIO PCI Express Root Port 2a (rev 06) | IIO #0 |
| 00 | 03 | 8086 | 3c08 | 0 | PCI bridge: Intel Corporation Xeon E5/Core i7 IIO PCI Express Root Port 3a in PCI Express Mode (rev 06) | IIO #0 |
| 00 | 05 | 8086 | 3c28 | 0 | System peripheral: Intel Corporation Xeon E5/Core i7 Control Status and Global Errors (rev 06) | IIO #0 |
| 00 | 05 | 8086 | 3c2a | 2 | System peripheral: Intel Corporation Xeon E5/Core i7 Control Status and Global Errors (rev 06) | IIO #0 |
| 00 | 05 | 8086 | 3c2c | 4 | PIC: Intel Corporation Xeon E5/Core i7 I/O APIC (rev 06) | IIO #0 |
| 00 | 11 | 8086 | 1d3e | 0 | PCI bridge: Intel Corporation C600/X79 series chipset PCI Express Virtual Root Port (rev 06) | PCH |
| 00 | 16 | 8086 | 1d3a | 0 | Communication controller: Intel Corporation C600/X79 series chipset MEI Controller #1 (rev 05) | PCH |
| 00 | 16 | 8086 | 1d3b | 1 | Communication controller: Intel Corporation C600/X79 series chipset MEI Controller #2 (rev 05) | PCH |

| BUS# | DEV# | V. ID | D. ID | Funct. # | Description | PCI Description |
|---|---|---|---|---|---|---|
| 00 | 1a | 8086 | 1d2d | 0 | USB controller: Intel Corporation C600/X79 series chipset USB2 Enhanced Host Controller #2 (rev 06) | PCH |
| 00 | 1c | 8086 | 1d10 | 0 | PCI bridge: Intel Corporation C600/X79 series chipset PCI Express Root Port 1 (rev b6) | PCH |
| 00 | 1c | 8086 | 1d1e | 7 | PCI bridge: Intel Corporation C600/X79 series chipset PCI Express Root Port 8 (rev b6) | PCH |
| 00 | 1d | 8086 | 1d26 | 0 | USB controller: Intel Corporation C600/X79 series chipset USB2 Enhanced Host Controller #1 (rev 06) | PCH |
| 00 | 1e | 8086 | 244e | 0 | PCI bridge: Intel Corporation 82801 PCI Bridge (rev a6) | PCH |
| 00 | 1f | 8086 | 1d41 | 0 | ISA bridge: Intel Corporation C600/X79 series chipset LPC Controller (rev 06) | PCH |
| 00 | 1f | 8086 | 1d22 | 3 | SMBus: Intel Corporation C600/X79 series chipset SMBus Host Controller (rev 06) | PCH |
| 01 | 00 | 15b3 | 1003 | 0 | Ethernet controller: Mellanox Technologies MT27500 Family [ConnectX-3] | ConnectX-3 on Fabric Interface (CPU 0) |
| 02 | 00 | 8086 | 1d69 | 0 | Serial Attached SCSI controller: Intel Corporation C604/X79 series chipset 4-Port SATA/SAS Storage Control Unit (rev 06) | |
| 02 | 00 | 8086 | 1d70 | 3 | SMBus: Intel Corporation C600/X79 series SMBus Controller 0 (rev 6) | |
| 04 | 00 | 1912 | 0013 | 0 | PCI bridge: Renesas Technology Corp. SH7757 PCIe Switch [PS] | |
| 05 | 00 | 1912 | 0013 | 0 | PCI bridge: Renesas Technology Corp. SH7757 PCIe Switch [PS] | |
| 05 | 01 | 1912 | 0013 | 0 | PCI bridge: Renesas Technology Corp. SH7757 PCIe Switch [PS] | |
| 06 | 00 | 1912 | 0013 | 0 | PCI bridge: Renesas Technology Corp. SH7757 PCIe-PCI Bridge [PPB] | |
| 7f | 08 | 8086 | 3c80 | 0 | System peripheral: Intel Corporation Xeon E5/Core i7 QPI Link 0 (rev 06) | IIO #0 |
| 7f | 08 | 8086 | 3c83 | 3 | System peripheral: Intel Corporation Xeon E5/Core i7 QPI Link Reut 0 (rev 06) | IIO #0 |
| 7f | 08 | 8086 | 3c84 | 4 | System peripheral: Intel Corporation Xeon E5/Core i7 QPI Link Reut 0 (rev 06) | IIO #0 |
| 7f | 09 | 8086 | 3c90 | 0 | System peripheral: Intel Corporation Xeon E5/Core i7 QPI Link 1 (rev 06) | IIO #0 |
| 7f | 09 | 8086 | 3c93 | 3 | System peripheral: Intel Corporation Xeon E5/Core i7 QPI Link Reut 1 (rev 06) | IIO #0 |
| 7f | 09 | 8086 | 3c94 | 4 | System peripheral: Intel Corporation Xeon E5/Core i7 QPI Link Reut 1 (rev 06) | IIO #0 |
| 7f | 0a | 8086 | 3cc0 | 0 | System peripheral: Intel Corporation Xeon E5/Core i7 Power Control Unit 0 (rev 06) | IIO #0 |
| 7f | 0a | 8086 | 3cc1 | 1 | System peripheral: Intel Corporation Xeon E5/Core i7 Power Control Unit 1 (rev 06) | IIO #0 |
| 7f | 0a | 8086 | 3cc2 | 2 | System peripheral: Intel Corporation Xeon E5/Core i7 Power Control Unit 2 (rev 06) | IIO #0 |
| 7f | 0a | 8086 | 3cd0 | 3 | System peripheral: Intel Corporation Xeon E5/Core i7 Power Control Unit 3 (rev 06) | IIO #0 |

| BUS# | DEV# | V. ID | D. ID | Funct. # | Description | PCI Description |
|---|---|---|---|---|---|---|
| 7f | 0b | 8086 | 3ce0 | 0 | System peripheral: Intel Corporation Xeon E5/Core i7 Interrupt Control Registers (rev 06) | IIO #0 |
| 7f | 0b | 8086 | 3ce3 | 3 | System peripheral: Intel Corporation Xeon E5/Core i7 Semaphore and Scratchpad Configuration Registers (rev 06) | IIO #0 |
| 7f | 0c | 8086 | 3ce8 | 0 | System peripheral: Intel Corporation Xeon E5/Core i7 Unicast Register 0 (rev 06) | IIO #0 |
| 7f | 0c | 8086 | 3ce8 | 1 | System peripheral: Intel Corporation Xeon E5/Core i7 Unicast Register 0 (rev 06) | IIO #0 |
| 7f | 0c | 8086 | 3ce8 | 2 | System peripheral: Intel Corporation Xeon E5/Core i7 Unicast Register 0 (rev 06) | IIO #0 |
| 7f | 0c | 8086 | 3ce8 | 3 | System peripheral: Intel Corporation Xeon E5/Core i7 Unicast Register 0 (rev 06) | IIO #0 |
| 7f | 0c | 8086 | 3cf4 | 6 | System peripheral: Intel Corporation Xeon E5/Core i7 Integrated Memory Controller System Address Decoder 0 (rev 06) | IIO #0 |
| 7f | 0c | 8086 | 3cf6 | 7 | System peripheral: Intel Corporation Xeon E5/Core i7 System Address Decoder (rev 06) | IIO #0 |
| 7f | 0d | 8086 | 3ce8 | 0 | System peripheral: Intel Corporation Xeon E5/Core i7 Unicast Register 0 (rev 06) | IIO #0 |
| 7f | 0d | 8086 | 3ce8 | 1 | System peripheral: Intel Corporation Xeon E5/Core i7 Unicast Register 0 (rev 06) | IIO #0 |
| 7f | 0d | 8086 | 3ce8 | 2 | System peripheral: Intel Corporation Xeon E5/Core i7 Unicast Register 0 (rev 06) | IIO #0 |
| 7f | 0d | 8086 | 3ce8 | 3 | System peripheral: Intel Corporation Xeon E5/Core i7 Unicast Register 0 (rev 06) | IIO #0 |
| 7f | 0d | 8086 | 3cf5 | 6 | System peripheral: Intel Corporation Xeon E5/Core i7 Integrated Memory Controller System Address Decoder 1 (rev 06) | IIO #0 |
| 7f | 0e | 8086 | 3ca0 | 0 | System peripheral: Intel Corporation Xeon E5/Core i7 Processor Home Agent (rev 06) | IIO #0 |
| 7f | 0e | 8086 | 3c46 | 1 | Performance counters: Intel Corporation Xeon E5/Core i7 Processor Home Agent Performance Monitoring (rev 06) | IIO #0 |
| 7f | 0f | 8086 | 3ca8 | 0 | System peripheral: Intel Corporation Xeon E5/Core i7 Integrated Memory Controller Registers (rev 06) | IIO #0 |
| 7f | 0f | 8086 | 3c71 | 1 | System peripheral: Intel Corporation Xeon E5/Core i7 Integrated Memory Controller RAS Registers (rev 06) | IIO #0 |
| 7f | 0f | 8086 | 3caa | 2 | System peripheral: Intel Corporation Xeon E5/Core i7 Integrated Memory Controller Target Address Decoder 0 (rev 06) | IIO #0 |
| 7f | 0f | 8086 | 3cab | 3 | System peripheral: Intel Corporation Xeon E5/Core i7 Integrated Memory Controller Target Address Decoder 1 (rev 06) | IIO #0 |
| 7f | 0f | 8086 | 3cac | 4 | System peripheral: Intel Corporation Xeon E5/Core i7 Integrated Memory Controller Target Address Decoder 2 (rev 06) | IIO #0 |
| 7f | 0f | 8086 | 3cad | 5 | System peripheral: Intel Corporation Xeon E5/Core i7 Integrated Memory Controller Target Address Decoder 3 (rev 06) | IIO #0 |
| 7f | 0f | 8086 | 3cae | 6 | System peripheral: Intel Corporation Xeon E5/Core i7 Integrated Memory Controller Target Address Decoder 4 (rev 06) | IIO #0 |
| 7f | 10 | 8086 | 3cb0 | 0 | System peripheral: Intel Corporation Xeon E5/Core i7 Integrated Memory Controller Channel 0-3 Thermal Control 0 (rev 06) | IIO #0 |

| BUS# | DEV# | V. ID | D. ID | Funct. # | Description | PCI Description |
|---|---|---|---|---|---|---|
| 7f | 10 | 8086 | 3cb1 | 1 | System peripheral: Intel Corporation Xeon E5/Core i7 Integrated Memory Controller Channel 0-3 Thermal Control 1 (rev 06) | IIO #0 |
| 7f | 10 | 8086 | 3cb2 | 2 | System peripheral: Intel Corporation Xeon E5/Core i7 Integrated Memory Controller ERROR Registers 0 (rev 06) | IIO #0 |
| 7f | 10 | 8086 | 3cb3 | 3 | System peripheral: Intel Corporation Xeon E5/Core i7 Integrated Memory Controller ERROR Registers 1 (rev 06) | IIO #0 |
| 7f | 10 | 8086 | 3cb4 | 4 | System peripheral: Intel Corporation Xeon E5/Core i7 Integrated Memory Controller Channel 0-3 Thermal Control 2 (rev 06) | IIO #0 |
| 7f | 10 | 8086 | 3cb5 | 5 | System peripheral: Intel Corporation Xeon E5/Core i7 Integrated Memory Controller Channel 0-3 Thermal Control 3 (rev 06) | IIO #0 |
| 7f | 10 | 8086 | 3cb6 | 6 | System peripheral: Intel Corporation Xeon E5/Core i7 Integrated Memory Controller ERROR Registers 2 (rev 06) | IIO #0 |
| 7f | 10 | 8086 | 3cb7 | 7 | System peripheral: Intel Corporation Xeon E5/Core i7 Integrated Memory Controller ERROR Registers 3 (rev 06) | IIO #0 |
| 7f | 11 | 8086 | 3cb8 | 0 | System peripheral: Intel Corporation Xeon E5/Core i7 DDRIO (rev 06) | IIO #0 |
| 7f | 13 | 8086 | 3ce4 | 0 | System peripheral: Intel Corporation Xeon E5/Core i7 R2PCIe (rev 06) | IIO #0 |
| 7f | 13 | 8086 | 3c43 | 1 | Performance counters: Intel Corporation Xeon E5/Core i7 Ring to PCI Express Performance Monitor (rev 06) | IIO #0 |
| 7f | 13 | 8086 | 3ce6 | 4 | Performance counters: Intel Corporation Xeon E5/Core i7 QuickPath Interconnect Agent Ring Registers (rev 06) | IIO #0 |
| 7f | 13 | 8086 | 3c44 | 5 | Performance counters: Intel Corporation Xeon E5/Core i7 Ring to QuickPath Interconnect Link 0 Performance Monitor (rev 06) | IIO #0 |
| 7f | 13 | 8086 | 3c45 | 6 | System peripheral: Intel Corporation Xeon E5/Core i7 Ring to QuickPath Interconnect Link 1 Performance Monitor (rev 06) | IIO #0 |
| 80 | 01 | 8086 | 3c02 | 0 | PCI bridge: Intel Corporation Xeon E5/Core i7 IIO PCI Express Root Port 1a (rev 06) -> RTM | IIO #1 |
| 80 | 02 | 8086 | 3c04 | 0 | PCI bridge: Intel Corporation Xeon E5/Core i7 IIO PCI Express Root Port 2a (rev 06) | IIO #1 |
| 80 | 02 | 8086 | 3c06 | 2 | PCI bridge: Intel Corporation Xeon E5/Core i7 IIO PCI Express Root Port 2c (rev 06) -> I350 | IIO #1 |
| 80 | 02 | 8086 | 3c07 | 3 | PCI bridge: Intel Corporation Xeon E5/Core i7 IIO PCI Express Root Port 2d (rev 06) | IIO #1 |
| 80 | 05 | 8086 | 3c28 | 0 | System peripheral: Intel Corporation Xeon E5/Core i7 Address Map, VTd_Misc, System Management (rev 06) | IIO #1 |
| 80 | 05 | 8086 | 3c2a | 2 | System peripheral: Intel Corporation Xeon E5/Core i7 Control Status and Global Errors (rev 06) | IIO #1 |
| 80 | 05 | 8086 | 3c2c | 4 | PIC: Intel Corporation Xeon E5/Core i7 I/O APIC (rev 06) | IIO #1 |
| 8a | 00 | 15b3 | 1003 | 0 | Ethernet controller: Mellanox Technologies MT27500 Family [ConnectX-3] | ConnectX-3 Fabric Interface |
| 8b | 00 | 8086 | 10c9 | 0 | Ethernet controller: Intel Corporation 82576 Gigabit Network Connection (rev 01) | I82576 on Base Interface |

| BUS# | DEV# | V. ID | D. ID | Funct. # | Description | PCI Description |
|---|---|---|---|---|---|---|
| 8b | 00 | 8086 | 10c9 | 1 | Ethernet controller: Intel Corporation 82576 Gigabit Network Connection (rev 01) | I82576 on Base Interface |
| 8d | 00 | 8086 | 1521 | 0 | Ethernet controller: Intel Corporation I350 Gigabit Network Connection (rev 01) | |
| 8d | 00 | 8086 | 1521 | 1 | Ethernet controller: Intel Corporation I350 Gigabit Network Connection (rev 01) | |
| 8d | 00 | 8086 | 1521 | 2 | Ethernet controller: Intel Corporation I350 Gigabit Network Connection (rev 01) | |
| 8d | 00 | 8086 | 1521 | 3 | Ethernet controller: Intel Corporation I350 Gigabit Network Connection (rev 01) | |
| 82 | 00 | 8086 | | 0 | Buses 82 - 8a are reserved for RTM Hot-Plug | RTM |
| ff | 08 | 8086 | 3c80 | 0 | System peripheral: Intel Corporation Xeon E5/Core i7 QPI Link 0 (rev 06) | IIO #1 |
| ff | 08 | 8086 | 3c83 | 3 | System peripheral: Intel Corporation Xeon E5/Core i7 QPI Link Reut 0 (rev 06) | IIO #1 |
| ff | 08 | 8086 | 3c84 | 4 | System peripheral: Intel Corporation Xeon E5/Core i7 QPI Link Reut 0 (rev 06) | IIO #1 |
| ff | 09 | 8086 | 3c90 | 0 | System peripheral: Intel Corporation Xeon E5/Core i7 QPI Link 1 (rev 06) | IIO #1 |
| ff | 09 | 8086 | 3c93 | 3 | System peripheral: Intel Corporation Xeon E5/Core i7 QPI Link Reut 1 (rev 06) | IIO #1 |
| ff | 09 | 8086 | 3c94 | 4 | System peripheral: Intel Corporation Xeon E5/Core i7 QPI Link Reut 1 (rev 06) | IIO #1 |
| ff | 0a | 8086 | 3cc0 | 0 | System peripheral: Intel Corporation Xeon E5/Core i7 Power Control Unit 0 (rev 06) | IIO #1 |
| ff | 0a | 8086 | 3cc1 | 1 | System peripheral: Intel Corporation Xeon E5/Core i7 Power Control Unit 1 (rev 06) | IIO #1 |
| ff | 0a | 8086 | 3cc2 | 2 | System peripheral: Intel Corporation Xeon E5/Core i7 Power Control Unit 2 (rev 06) | IIO #1 |
| ff | 0a | 8086 | 3cd0 | 3 | System peripheral: Intel Corporation Xeon E5/Core i7 Power Control Unit 3 (rev 06) | IIO #1 |
| ff | 0b | 8086 | 3ce0 | 0 | System peripheral: Intel Corporation Xeon E5/Core i7 Interrupt Control Registers (rev 06) | IIO #1 |
| ff | 0b | 8086 | 3ce3 | 3 | System peripheral: Intel Corporation Xeon E5/Core i7 Semaphore and Scratchpad Configuration Registers (rev 06) | IIO #1 |
| ff | 0c | 8086 | 3ce8 | 0 | System peripheral: Intel Corporation Xeon E5/Core i7 Unicast Register 0 (rev 06) | IIO #1 |
| ff | 0c | 8086 | 3ce8 | 1 | System peripheral: Intel Corporation Xeon E5/Core i7 Unicast Register 0 (rev 06) | IIO #1 |
| ff | 0c | 8086 | 3ce8 | 2 | System peripheral: Intel Corporation Xeon E5/Core i7 Unicast Register 0 (rev 06) | IIO #1 |
| ff | 0c | 8086 | 3ce8 | 3 | System peripheral: Intel Corporation Xeon E5/Core i7 Unicast Register 0 (rev 06) | IIO #1 |
| ff | 0c | 8086 | 3cf4 | 6 | System peripheral: Intel Corporation Xeon E5/Core i7 Integrated Memory Controller System Address Decoder 0 (rev 06) | IIO #1 |
| ff | 0c | 8086 | 3cf6 | 7 | System peripheral: Intel Corporation Xeon E5/Core i7 System Address Decoder (rev 06) | IIO #1 |

| BUS# | DEV# | V. ID | D. ID | Funct. # | Description | PCI Description |
|---|---|---|---|---|---|---|
| ff | 0d | 8086 | 3ce8 | 0 | System peripheral: Intel Corporation Xeon E5/Core i7 Unicast Register 0 (rev 06) | IIO #1 |
| ff | 0d | 8086 | 3ce8 | 1 | System peripheral: Intel Corporation Xeon E5/Core i7 Unicast Register 0 (rev 06) | IIO #1 |
| ff | 0d | 8086 | 3ce8 | 2 | System peripheral: Intel Corporation Xeon E5/Core i7 Unicast Register 0 (rev 06) | IIO #1 |
| ff | 0d | 8086 | 3ce8 | 3 | System peripheral: Intel Corporation Xeon E5/Core i7 Unicast Register 0 (rev 06) | IIO #1 |
| ff | 0d | 8086 | 3cf5 | 6 | System peripheral: Intel Corporation Xeon E5/Core i7 Integrated Memory Controller System Address Decoder 1 (rev 06) | IIO #1 |
| ff | 0e | 8086 | 3ca0 | 0 | System peripheral: Intel Corporation Xeon E5/Core i7 Processor Home Agent (rev 06) | IIO #1 |
| ff | 0e | 8086 | 3c46 | 1 | Performance counters: Intel Corporation Xeon E5/Core i7 Processor Home Agent Performance Monitoring (rev 06) | IIO #1 |
| ff | 0f | 8086 | 3ca8 | 0 | System peripheral: Intel Corporation Xeon E5/Core i7 Integrated Memory Controller Registers (rev 06) | IIO #1 |
| ff | 0f | 8086 | 3c71 | 1 | System peripheral: Intel Corporation Xeon E5/Core i7 Integrated Memory Controller RAS Registers (rev 06) | IIO #1 |
| ff | 0f | 8086 | 3caa | 2 | System peripheral: Intel Corporation Xeon E5/Core i7 Integrated Memory Controller Target Address Decoder 0 (rev 06) | IIO #1 |
| ff | 0f | 8086 | 3cab | 3 | System peripheral: Intel Corporation Xeon E5/Core i7 Integrated Memory Controller Target Address Decoder 1 (rev 06) | IIO #1 |
| ff | 0f | 8086 | 3cac | 4 | System peripheral: Intel Corporation Xeon E5/Core i7 Integrated Memory Controller Target Address Decoder 2 (rev 06) | IIO #1 |
| ff | 0f | 8086 | 3cad | 5 | System peripheral: Intel Corporation Xeon E5/Core i7 Integrated Memory Controller Target Address Decoder 3 (rev 06) | IIO #1 |
| ff | 0f | 8086 | 3cae | 6 | System peripheral: Intel Corporation Xeon E5/Core i7 Integrated Memory Controller Target Address Decoder 4 (rev 06) | IIO #1 |
| ff | 10 | 8086 | 3cb0 | 0 | System peripheral: Intel Corporation Xeon E5/Core i7 Integrated Memory Controller Channel 0-3 Thermal Control 0 (rev 06) | IIO #1 |
| ff | 10 | 8086 | 3cb1 | 1 | System peripheral: Intel Corporation Xeon E5/Core i7 Integrated Memory Controller Channel 0-3 Thermal Control 1 (rev 06) | IIO #1 |
| ff | 10 | 8086 | 3cb2 | 2 | System peripheral: Intel Corporation Xeon E5/Core i7 Integrated Memory Controller ERROR Registers 0 (rev 06) | IIO #1 |
| ff | 10 | 8086 | 3cb3 | 3 | System peripheral: Intel Corporation Xeon E5/Core i7 Integrated Memory Controller ERROR Registers 1 (rev 06) | IIO #1 |
| ff | 10 | 8086 | 3cb4 | 4 | System peripheral: Intel Corporation Xeon E5/Core i7 Integrated Memory Controller Channel 0-3 Thermal Control 2 (rev 06) | IIO #1 |
| ff | 10 | 8086 | 3cb5 | 5 | System peripheral: Intel Corporation Xeon E5/Core i7 Integrated Memory Controller Channel 0-3 Thermal Control 3 (rev 06) | IIO #1 |
| ff | 10 | 8086 | 3cb6 | 6 | System peripheral: Intel Corporation Xeon E5/Core i7 Integrated Memory Controller ERROR Registers 2 (rev 06) | IIO #1 |
| ff | 10 | 8086 | 3cb7 | 7 | System peripheral: Intel Corporation Xeon E5/Core i7 Integrated Memory Controller ERROR Registers 3 (rev 06) | IIO #1 |

| BUS# | DEV# | V. ID | D. ID | Funct. # | Description | PCI Description |
|---|---|---|---|---|---|---|
| ff | 11 | 8086 | 3cb8 | 0 | System peripheral: Intel Corporation Xeon E5/Core i7 DDRIO (rev 06) | IIO #1 |
| ff | 13 | 8086 | 3ce4 | 0 | System peripheral: Intel Corporation Xeon E5/Core i7 R2PCIe (rev 06) | IIO #1 |
| ff | 13 | 8086 | 3c43 | 1 | Performance counters: Intel Corporation Xeon E5/Core i7 Ring to PCI Express Performance Monitor (rev 06) | IIO #1 |
| ff | 13 | 8086 | 3ce6 | 4 | Performance counters: Intel Corporation Xeon E5/Core i7 QuickPath Interconnect Agent Ring Registers (rev 06) | IIO #1 |
| ff | 13 | 8086 | 3c44 | 5 | Performance counters: Intel Corporation Xeon E5/Core i7 Ring to QuickPath Interconnect Link 0 Performance Monitor (rev 06) | IIO #1 |
| ff | 13 | 8086 | 3c45 | 6 | System peripheral: Intel Corporation Xeon E5/Core i7 Ring to QuickPath Interconnect Link 1 Performance Monitor (rev 06) | IIO #1 |

# B. Connector Pinouts

## B.1 Connectors and Headers Summary

| Description | Connector | Comments |
|---|---|---|
| Memory Sockets | J1 -J8 | DDR3 1600 MHz Memory Sockets |
| USB Flash Connectors | J14 | USB Connectors for the eUSB Modules |
| USB Connectors | J10 | Dual USB Connector |
| Management Console Port | J11 | RJ-45 Serial Port Connector |
| 1GigE RJ45 Connectors | J12 & J13 | Face plate RJ45 Connectors |
| Base & Fabric Interface Connector | J23 & J23 | Base & Fabric Interface Connectors |
| RTM Connectors | J30 & J31 | RTM Connectors |
| SAS HDD/SDD Connectors | J16 | SAS/SATA HDD/SSD Connector |
| Power Connector | P10 | Power & IPMB |
| SW2 | Reset Switch | Reset Button |
| SW3 | User Switch | User button |

## B.2 USB Connectors (J10)

| Signal | Pin |
|---|---|
| A1 VCC | B1 VCC |
| A2 USB_DATA- | B2 USB_DATA- |
| A3 USB_DATA+ | B3 USB_DATA+ |
| A4 GND | B4 GND |

## B.3 Management Console Port (J11)

| Signal | Pin | | Pin | Signal |
|---|---|---|---|---|
| RTS | 1 | | 5 | GND |
| DTR | 2 | | 6 | RX# |
| TX# | 3 | | 7 | DSR |
| GND | 4 | | 8 | CTS |

## B.4 eUSB Flash Drive (J14)

| Signal | Pin | | Pin | Signal |
|---|---|---|---|---|
| VCC | 1 | | 6 | N.C. |
| N.C. | 2 | | 7 | GND |
| USB_DATA- | 3 | | 8 | N.C. |
| N.C. | 4 | | 9 | N.C. (Key) |
| USB_DATA+ | 5 | | 10 | N.C. |

## B.5 Fabric Interface (J22)

| Pin | ROW A | ROW B | ROW C | ROW D | ROW E | ROW F |
|---|---|---|---|---|---|---|
| 1 | N.C. | N.C. | N.C. | N.C. | N.C. | N.C. |
| 2 | N.C. | N.C. | N.C. | N.C. | N.C. | N.C. |
| 3 | N.C. | N.C. | N.C. | N.C. | N.C. | N.C. |
| 4 | N.C. | N.C. | N.C. | N.C. | N.C. | N.C. |
| 5 | N.C. | N.C. | N.C. | N.C. | N.C. | N.C. |
| 6 | N.C. | N.C. | N.C. | N.C. | N.C. | N.C. |
| 7 | Tx2[4]+ | Tx2[4]- | Rx2[4]+ | Rx2[4]- | Tx3[4]+ | Tx3[4]- |
| 8 | Tx0[4]+ | Tx0[4]- | Rx0[4]+ | Rx0[4]- | Tx1[4]+ | Tx1[4]- |
| 9 | Tx2[3]+ | Tx2[3]- | Rx2[3]+ | Rx2[3]- | Tx3[3]+ | Tx3[3]- |
| 10 | Tx0[3]+ | Tx0[3]- | Rx0[3]+ | Rx0[3]- | Tx1[3]+ | Tx1[3]- |

| Pin | ROW G | ROW H | ROW AB | ROW CD | ROW EF | ROW GH |
|---|---|---|---|---|---|---|
| 1 | N.C. | N.C. | GND | GND | GND | GND |
| 2 | N.C. | N.C. | GND | GND | GND | GND |
| 3 | N.C. | N.C. | GND | GND | GND | GND |
| 4 | N.C. | N.C. | GND | GND | GND | GND |
| 5 | N.C. | N.C. | GND | GND | GND | GND |
| 6 | N.C. | N.C. | GND | GND | GND | GND |
| 7 | Rx3[4]+ | Rx3[4]- | GND | GND | GND | GND |
| 8 | Rx1[4]+ | Rx1[4]- | GND | GND | GND | GND |
| 9 | Rx3[3]+ | Rx3[3]- | GND | GND | GND | GND |
| 10 | Rx1[3]+ | Rx1[3]- | GND | GND | GND | GND |

# B.6 Base Interface & Fabric Interface (J23)

| Pin | ROW A | ROW B | ROW C | ROW D | ROW E | ROW F |
|---|---|---|---|---|---|---|
| 1 | Tx2[2]+ | Tx2[2]- | Rx2[2]+ | Rx2[2]- | Tx3[2]+ | Tx3[2]- |
| 2 | Tx0[2]+ | Tx0[2]- | Rx0[2]+ | Rx0[2]- | Tx1[2]+ | Tx1[2]- |
| 3 | Tx2[1]+ | Tx2[1]- | Rx2[1]+ | Rx2[1]- | Tx3[1]+ | Tx3[1]- |
| 4 | Tx0[1]+ | Tx0[1]- | Rx0[1]+ | Rx0[1]- | Tx1[1]+ | Tx1[1]- |
| 5 | BI_DA1+ | BI_DA1- | BI_DB1+ | BI_DB1- | BI_DC1+ | BI_DC1- |
| 6 | BI_DA2+ | DI_DA2- | BI_DB2+ | BI_DB2- | DI_DC2+ | BI_DC2- |
| 7 | N.C. | N.C. | N.C. | N.C. | N.C. | N.C. |
| 8 | N.C. | N.C. | N.C. | N.C. | N.C. | N.C. |
| 9 | N.C. | N.C. | N.C. | N.C. | N.C. | N.C. |
| 10 | N.C. | N.C. | N.C. | N.C. | N.C. | N.C. |

| Pin | ROW G | ROW H | ROW AB | ROW CD | ROW EF | ROW GH |
|---|---|---|---|---|---|---|
| 1 | Rx3[2]+ | Rx3[2]- | GND | GND | GND | GND |
| 2 | Rx1[2]+ | Rx1[2]- | GND | GND | GND | GND |
| 3 | Rx3[1]+ | Rx3[1]- | GND | GND | GND | GND |
| 4 | Rx1[1]+ | Rx1[1]- | GND | GND | GND | GND |
| 5 | BI_DD1+ | BI_DD1- | GND | GND | GND | GND |
| 6 | BI_DD2+ | DI_DD2- | GND | GND | GND | GND |
| 7 | N.C. | N.C. | GND | GND | GND | GND |
| 8 | N.C. | N.C. | GND | GND | GND | GND |
| 9 | N.C. | N.C. | GND | GND | GND | GND |
| 10 | N.C. | N.C. | GND | GND | GND | GND |

# B.7 RTM Connector (J30)

| Pin | ROW A | ROW B | ROW C | ROW D | ROW E | ROW F |
|---|---|---|---|---|---|---|
| 1 | V_12V_1 | V_12V_5 | V_12V_2 | V_3V3_SUS | FGPIO1 | RTM_PRSNT# |
| 2 | V_12V_3 | V_12V_6 | V_12V_4 | N.C._D2 | IPMC_SCL | IPMC_SDA |
| 3 | SP_TX | SP_RX | JTAG_TDI | JTAG_TDO | JTAG_TMS | JTAG_TCK |
| 4 | USB1_D+ | USB1_D- | INT_0 | INT_1 | RTML_TX | RTML_RX |
| 5 | SP_RTS# | SP_CTS# | MD2# | RSVD_D5 | CLK_PE+ | CLK_PE- |
| 6 | SATA_TX+ | SATA_TX- | SATA_RX+ | SATA_RX- | SFP1_SCL | SFP1_SDA |
| 7 | N.C. | N.C. | N.C. | N.C. | N.C. | N.C. |
| 8 | GBE_TX1+ | GBE_TX1- | GBE_RX1+ | GBE_RX1- | GBE_TX2+ | GBE_TX2- |
| 9 | PE6_TX- | PE6_TX+ | PE7_RX- | PE7_RX+ | PE5_TX+ | PE5_TX- |
| 10 | PE4_TX- | PE4_TX+ | PE5_RX+ | PE5_RX- | PE7_TX+ | PE7_TX- |

| Pin | ROW G | ROW H | ROW AB | ROW CD | ROW EF | ROW GH |
|---|---|---|---|---|---|---|
| 1 | RTM_PCIRST # | RTM_EN# | GND | GND | GND | GND |
| 2 | USB0_D+ | USB0_D- | GND | GND | GND | GND |
| 3 | JTAG_TRST | FGPIO0 | GND | GND | GND | GND |
| 4 | RTML_CLK | PROG | GND | GND | GND | GND |
| 5 | RSVD_G5 | JTAG_SEL | GND | GND | GND | GND |
| 6 | SFP0_SCL | SFP0_SDA | GND | GND | GND | GND |
| 7 | N.C. | N.C. | GND | GND | GND | GND |
| 8 | GBE_RX2+ | GBE_RX2- | GND | GND | GND | GND |
| 9 | PE6_RX+ | PE6_RX- | GND | GND | GND | GND |
| 10 | PE4_RX- | PE4_RX+ | GND | GND | GND | GND |

# B.8 RTM Connector (J31)

| Pin | ROW A | ROW B | ROW C | ROW D | ROW E | ROW F |
|---|---|---|---|---|---|---|
| 1 | N.C. | N.C. | N.C. | N.C. | N.C. | N.C. |
| 2 | N.C. | N.C. | N.C. | N.C. | N.C. | N.C. |
| 3 | N.C. | N.C. | N.C. | N.C. | N.C. | N.C. |
| 4 | N.C. | N.C. | N.C. | N.C. | N.C. | N.C. |
| 5 | PE2_TX+ | PE2_TX- | PE3_RX+ | PE3_RX- | PE1_TX+ | PE1_TX- |
| 6 | PE0_TX+ | PE0_TX- | PE1_RX- | PE1_RX+ | PE3_TX+ | PE3_TX- |
| 7 | SAS2_TX+ | SAS2_TX- | SAS2_RX+ | SAS2_RX- | N.C. | N.C. |
| 8 | N.C. | N.C. | N.C. | N.C. | SAS0_TX+ | SAS0_TX- |
| 9 | N.C. | N.C. | N.C. | N.C. | DDC_SCL_5V | DDC_SDA_5V |
| 10 | CLK_PE1+ | CLK_PE1- | N.C. | N.C. | HSYNCB | VSYNCB |

| Pin | ROW G | ROW H | ROW AB | ROW CD | ROW EF | ROW GH |
|---|---|---|---|---|---|---|
| 1 | N.C. | N.C. | GND | GND | GND | GND |
| 2 | N.C. | N.C. | GND | GND | GND | GND |
| 3 | N.C. | N.C. | GND | GND | GND | GND |
| 4 | N.C. | N.C. | GND | GND | GND | GND |
| 5 | PE2_RX- | PE2_RX+ | GND | GND | GND | GND |
| 6 | PE0_RX- | PE0_RX- | GND | GND | GND | GND |
| 7 | N.C. | N.C. | GND | GND | GND | GND |
| 8 | SAS0_RX+ | SAS0_RX- | GND | GND | GND | GND |
| 9 | N.C. | BLUE | GND | GND | GND | GND |
| 10 | RED | GREEN | GND | GND | GND | GND |

## B.9 Power (P10)

| Signal | Pin | | Pin | Signal |
|---|---|---|---|---|
| N.C. | 1 | | 2 | N.C. |
| N.C. | 3 | | 4 | N.C. |
| HA0 | 5 | | 6 | HA1 |
| HA2 | 7 | | 8 | HA3 |
| HA4 | 9 | | 10 | HA5 |
| HA6 | 11 | | 12 | HA7/P |
| SCL_A | 13 | | 14 | SDA_A |
| SCL_B | 15 | | 16 | SDA_B |
| MT1_TIP(N.C.) | 17 | | 18 | MT2_TIP(N.C.) |
| RING_A(N.C.) | 19 | | 20 | RING_B(N.C.) |
| MT1_RING(N.C.) | 21 | | 22 | MT2_RING(N.C.) |
| RRTN_A(N.C.) | 23 | | 24 | RRTN_B(N.C.) |
| SHELF_GND | 25 | | 26 | LOGIC_GND |
| ENABLE_B | 27 | | 28 | VRTN_A |
| VRTN_B | 29 | | 30 | EARLY_A (N.C.) |
| EARLY_B (N.C.) | 31 | | 32 | ENABLE_A |
| -48V_A | 33 | | 34 | -48V_B |

# C. BIOS Setup Error Codes

## C.1 Memory Reference Code

### C.1.1 Progress Codes

| Code | Description |
|---|---|
| 0B0h | Detect DIMM population |
| 0B1h | Set DDR3 frequency |
| 0B2h | Gather remaining SPD data |
| 0B3h | Program registers on the memory controller level |
| 0B4h | Evaluate RAS modes and save rank information |
| 0B5h | Program registers on the channel level |
| 0B6h | Perform the JEDEC defined initialization sequence |
| 0B7h | Train DDR3 ranks |
| 0B8h | Initialize CLTT/OLTT |
| 0B9h | Hardware memory test and init |
| 0BAh | Execute software memory init |
| 0BBh | Program memory map and interleaving |
| 0BCh | Program RAS configuration |
| 0BFh | MRC is done |

### C.1.2 Error Codes

| Code | Description |
|---|---|
| 0E8h | No Memory |
| 0E9h | Memory is locked by LT, inaccessible. |
| 0EAh | DDR3 training did complete successfully |
| 0EBh | Memory test failure |
| 0EDh | UDIMMs and RDIMMs are both present DIMM vendor-specific errors |

# C.2 SEC Status Codes

| Status Code | Description |
|---|---|
| 0x0 | Not Used |
| 0x1 | Power on. Reset type detection (soft/hard) |
| 0x2 | AP initialization before microcode loading |
| 0x3 | North Bridge initialization before microcode loading |
| 0x4 | South Bridge initialization before microcode loading |
| 0x5 | OEM initialization before microcode loading |
| 0x6 | Microcode loading |
| 0x7 | AP initialization after microcode loading |
| 0x8 | North Bridge initialization after microcode loading |
| 0x9 | South Bridge initialization after microcode loading |
| 0xA | OEM initializataion after microcode loading |
| 0xB | Cache initialization |
| 0xC - 0xD | Reserved for future AMI SEC error codes |
| 0xE | Microcode not found |
| 0xF | Microcode not loaded |

# C.3 PEI Status Codes

| Status Code | Description |
|---|---|
| 0x10 | PEI Core is started |
| 0x11 | Pre-memory CPU initialization is started |
| 0x12 | Pre-memory CPU initialization (CPU module specific) |
| 0x13 | Pre-memory CPU initialization (CPU module specific) |
| 0x14 | Pre-memory CPU initialization (CPU module specific) |
| 0x15 | Pre-memory North Bridge initialization is started |
| 0x16 | Pre-Memory North Bridge initialization (North Bridge module specific) |
| 0x17 | Pre-Memory North Bridge initialization (North Bridge module specific) |
| 0x18 | Pre-Memory North Bridge initialization (North Bridge module specific) |
| 0x19 | Pre-memory South Bridge initialization is started |
| 0x1A | Pre-memory South Bridge initialization (South Bridge module specific) |
| 0x1B | Pre-memory South Bridge initialization (South Bridge module specific) |
| 0x1C | Pre-memory South Bridge initialization (South Bridge module specific) |
| 0x1D - 0x2A | OEM pre-memory initialization codes |
| 0x2B | Memory initialization. Serial Presence Detect (SPD) data reading |
| 0x2C | Memory initialization. Memory presence detection |
| 0x2D | Memory initialization. Programming memory timing information |
| 0x2E | Memory initialization. Configuring memory |

| Status Code | Description |
|---|---|
| 0x2F | Memory initialization (other). |
| 0x30 | Reserved for ASL (see ASL Status Codes section below) |
| 0x31 | Memory Installed |
| 0x32 | CPU post-memory initialization is started |
| 0x33 | CPU post-memory initialization. Cache initialization |
| 0x34 | CPU post-memory initialization. Application Processor(s) (AP) initialization |
| 0x35 | CPU post-memory initialization. Boot Strap Processor (BSP) selection |
| 0x36 | CPU post-memory initialization. System Management Mode (SMM) initialization |
| 0x37 | Post-Memory North Bridge initialization is started |
| 0x38 | Post-Memory North Bridge initialization (North Bridge module specific) |
| 0x39 | Post-Memory North Bridge initialization (North Bridge module specific) |
| 0x3A | Post-Memory North Bridge initialization (North Bridge module specific) |
| 0x3B | Post-Memory South Bridge initialization is started |
| 0x3C | Post-Memory South Bridge initialization (South Bridge module specific) |
| 0x3D | Post-Memory South Bridge initialization (South Bridge module specific) |
| 0x3E | Post-Memory South Bridge initialization (South Bridge module specific) |
| 0x3F - 0x4E | OEM post memory initialization codes |
| 0x4F | DXE IPL is started |
| 0x50 | Memory initialization error. Invalid memory type or incompatible memory speed |
| 0x51 | Memory initialization error. SPD reading has failed |
| 0x52 | Memory initialization error. Invalid memory size or memory modules do not match. |
| 0x53 | Memory initialization error. No usable memory detected |
| 0x54 | Unspecified memory initialization error. |
| 0x55 | Memory not installed |
| 0x56 | Invalid CPU type or Speed |
| 0x57 | CPU mismatch |
| 0x58 | CPU self test failed or possible CPU cache error |
| 0x59 | CPU micro-code is not found or micro-code update is failed |
| 0x5A | Internal CPU error |
| 0x5B | reset PPI is not available |
| 0x5C - 0x5F | Reserved for future AMI error codes |
| 0xE0 | S3 Resume is stared (S3 Resume PPI is called by the DXE IPL) |
| 0xE1 | S3 Boot Script execution |
| 0xE2 | Video repost |
| 0xE3 | OS S3 wake vector call |
| 0xE4 - 0xE7 | Reserved for future AMI progress codes |
| 0xE8 | S3 Resume Failed in PEI |
| 0xE9 | S3 Resume PPI not Found |
| 0xEA | S3 Resume Boot Script Error |
| 0xEB | S3 OS Wake Error |
| 0xEC-0xEF | Reserved for future AMI error codes |
| 0xF0 | Recovery condition triggered by firmware (Auto recovery) |

| Status Code | Description |
|---|---|
| 0xF1 | Recovery condition triggered by user (Forced recovery) |
| 0xF2 | Recovery process started |
| 0xF3 | Recovery firmware image is found |
| 0xF4 | Recovery firmware image is loaded |
| 0xF5-0xF7 | Reserved for future AMI progress codes |
| 0xF8 | Recovery PPI is not available |
| 0xF9 | Recovery capsule is not found |
| 0xFA | Invalid recovery capsule |
| 0xFB – 0xFF | Reserved for future AMI error codes |

# C.4 DXE Status Codes

| Status Code | Description |
|---|---|
| 0x60 | DXE Core is started |
| 0x61 | NVRAM initialization |
| 0x62 | Installation of the South Bridge Runtime Services |
| 0x63 | CPU DXE initialization is started |
| 0x64 | CPU DXE initialization (CPU module specific) |
| 0x65 | CPU DXE initialization (CPU module specific) |
| 0x66 | CPU DXE initialization (CPU module specific) |
| 0x67 | CPU DXE initialization (CPU module specific) |
| 0x68 | PCI host bridge initialization |
| 0x69 | North Bridge DXE initialization is started |
| 0x6A | North Bridge DXE SMM initialization is started |
| 0x6B | North Bridge DXE initialization (North Bridge module specific) |
| 0x6C | North Bridge DXE initialization (North Bridge module specific) |
| 0x6D | North Bridge DXE initialization (North Bridge module specific) |
| 0x6E | North Bridge DXE initialization (North Bridge module specific) |
| 0x6F | North Bridge DXE initialization (North Bridge module specific) |
| 0x70 | South Bridge DXE initialization is started |
| 0x71 | South Bridge DXE SMM initialization is started |
| 0x72 | South Bridge devices initialization |
| 0x73 | South Bridge DXE Initialization (South Bridge module specific) |
| 0x74 | South Bridge DXE Initialization (South Bridge module specific) |
| 0x75 | South Bridge DXE Initialization (South Bridge module specific) |
| 0x76 | South Bridge DXE Initialization (South Bridge module specific) |
| 0x77 | South Bridge DXE Initialization (South Bridge module specific) |
| 0x78 | ACPI module initialization |
| 0x79 | CSM initialization |
| 0x7A – 0x7F | Reserved for future AMI DXE codes |

| Status Code | Description |
|---|---|
| 0x80 – 0x8F | OEM DXE initialization codes |
| 0x90 | Boot Device Selection (BDS) phase is started |
| 0x91 | Driver connecting is started |
| 0x92 | PCI Bus initialization is started |
| 0x93 | PCI Bus Hot Plug Controller Initialization |
| 0x94 | PCI Bus Enumeration |
| 0x95 | PCI Bus Request Resources |
| 0x96 | PCI Bus Assign Resources |
| 0x97 | Console Output devices connect |
| 0x98 | Console input devices connect |
| 0x99 | Super IO Initialization |
| 0x9A | USB initialization is started |
| 0x9B | USB Reset |
| 0x9C | USB Detect |
| 0x9D | USB Enable |
| 0x9E – 0x9F | Reserved for future AMI codes |
| 0xA0 | IDE initialization is started |
| 0xA1 | IDE Reset |
| 0xA2 | IDE Detect |
| 0xA3 | IDE Enable |
| 0xA4 | SCSI initialization is started |
| 0xA5 | SCSI Reset |
| 0xA6 | SCSI Detect |
| 0xA7 | SCSI Enable |
| 0xA8 | Setup Verifying Password |
| 0xA9 | Start of Setup |
| 0xAA | Reserved for ASL (see ASL Status Codes section below) |
| 0xAB | Setup Input Wait |
| 0xAC | Reserved for ASL (see ASL Status Codes section below) |
| 0xAD | Ready To Boot event |
| 0xAE | Legacy Boot event |
| 0xAF | Exit Boot Services event |
| 0xB0 | Runtime Set Virtual Address MAP Begin |
| 0xB1 | Runtime Set Virtual Address MAP End |
| 0xB2 | Legacy Option ROM Initialization |
| 0xB3 | System Reset |
| 0xB4 | USB hot plug |
| 0xB5 | PCI bus hot plug |
| 0xB6 | Clean-up of NVRAM |
| 0xB7 | Configuration Reset (reset of NVRAM settings) |
| 0xB8 – 0xBF | Reserved for future AMI codes |
| 0xC0 – 0xCF | OEM BDS initialization codes |

| Status Code | Description |
|---|---|
| 0xD0 | CPU initialization error |
| 0xD1 | North Bridge initialization error |
| 0xD2 | South Bridge initialization error |
| 0xD3 | Some of the Architectural Protocols are not available |
| 0xD4 | PCI resource allocation error. Out of Resources |
| 0xD5 | No Space for Legacy Option ROM |
| 0xD6 | No Console Output Devices are found |
| 0xD7 | No Console Input Devices are found |
| 0xD8 | Invalid password |
| 0xD9 | Error loading Boot Option (LoadImage returned error) |
| 0xDA | Boot Option is failed (StartImage returned error) |
| 0xDB | Flash update is failed |
| 0xDC | Reset protocol is not available |

## C.5 ACPI/ASL Status Codes

| Status Code | Description |
|---|---|
| 0x01 | System is entering S1 sleep state |
| 0x02 | System is entering S2 sleep state |
| 0x03 | System is entering S3 sleep state |
| 0x04 | System is entering S4 sleep state |
| 0x05 | System is entering S5 sleep state |
| 0x10 | System is waking up from the S1 sleep state |
| 0x20 | System is waking up from the S2 sleep state |
| 0x30 | System is waking up from the S3 sleep state |
| 0x40 | System is waking up from the S4 sleep state |
| 0xAC | System has transitioned into ACPI mode. Interrupt controller is in PIC mode. |
| 0xAA | System has transitioned into ACPI mode. Interrupt controller is in APIC mode. |

# D. Software Update

To update the board software, it is recommended to use the Kontron HPM bundle. Depending on the component(s) updated, a payload reset may be required to activate the newly uploaded firmware.

HPM Bundles can be applied using the Web Management Interface (see section xxxx) or using ipmitool hpm commands (see ipmitool help documentation for more details).

The latest versions of the HPM bundles are available from the Kontron Canada's website (cbu.kontron.ca)

# E. Getting Help

If, at any time, you encounter difficulties with your application or with any of our products, or if you simply need guidance on system setups and capabilities, contact our Technical Support at:

| North America | EMEA |
|---|---|
| Tel.: (450) 437-5682 | Tel.: +49 (0) 8341 803 333 |
| Fax: (450) 437-8053 | Fax: +49 (0) 8341 803 339 |

If you have any questions about Kontron, our products, or services, visit our Web site at: www.kontron.com

You also can contact us by E-mail at:

North America: support@ca.kontron.com

EMEA: support-kom@kontron.com

Or at the following address:

| North America | EMEA |
|---|---|
| Kontron Canada, Inc. | Kontron Modular Computers GmbH |
| 4555, Ambroise-Lafortune | Sudetenstrasse 7 |
| Boisbriand, Québec | 87600 Kaufbeuren |
| J7H 0A4 Canada | Germany |

## E.1 Returning Defective Merchandise

Before returning any merchandise please do one of the following:

- Call

    1) Call our Technical Support department in North America at (450) 437-5682 and in EMEA at +49 (0) 8341 803 333. Make sure you have the following on hand: our Invoice #, your Purchase Order #, and the Serial Number of the defective unit.

    2) Provide the serial number found on the back of the unit and explain the nature of your problem to a service technician.

3) The technician will instruct you on the return procedure if the problem cannot be solved over the telephone.

4) Make sure you receive an RMA # from our Technical Support before returning any merchandise.

- E-mail

1) Send us an e-mail at: RMA@ca.kontron.com in North America and at: orderprocessing@kontron-modular.com in EMEA. In the e-mail, you must include your name, your company name, your address, your city, your postal/zip code, your phone number, and your e-mail. You must also include the serial number of the defective product and a description of the problem.

## E.2 When Returning a Unit

- In the box, you must include the name and telephone number of a contact person, in case further explanations are required. Where applicable, always include all duty papers and invoice(s) associated with the item(s) in question.
- Ensure that the unit is properly packed. Pack it in a rigid cardboard box.
- Clearly write or mark the RMA number on the outside of the package you are returning.
- Ship prepaid. We take care of insuring incoming units.

| North America | EMEA |
|---|---|
| Kontron Canada, Inc. | Kontron Modular Computers GmbH |
| 4555, Ambroise-Lafortune | Sudetenstrasse 7 |
| Boisbriand, Québec | 87600 Kaufbeuren |
| J7H 0A4 Canada | Germany |

# F. Glossary

| Acronyms | Descriptions |
|---|---|
| AC | Alternate Current |
| ACPI | Advanced Configuration & Power Interface |
| AHCI | Advanced Host Controller Interface |
| AMI | American Megatrends Inc |
| ANSI | American National Standards Institute |
| APIC | Advanced Programmable Interrupt Controller |
| ARI | Alternative Routing-ID Interpretation. Next generation I/O implementations to support an increased number of concurrent users of a multi-Function device |
| ASCII | American Standard Code for Information Interchange. ASCII codes represent text in computers, communications equipment, and other devices that work with text. |
| ASPM | Active State Power Management. A power management protocol used to manage PCI Express-based serial link devices. |
| ATA | Advanced Technology Attachment |
| ATCA | Advanced Telecommunications Computing Architecture |
| ATS | Address Translation Services. Set of transactions for PCI Express components to exchange and use translated addresses in support of native I/O Virtualization. |
| BBS | BIOS Boot Specification |
| BI | Base Interface. Backplane connectivity defined by the ATCA. |
| BIOS | Basic Input/Output System |
| BMC | Base Management Controller |
| BOM | Bill Of Material |
| BT | Block Transfer. An optional IPMI system management interface. |
| BW | BandWidth |
| CB | Certification Body |
| CD | Compact Disk |
| CDROM | (Same as CD-ROM). Compact Disk Read-Only Memory. |
| CE | Conformit?Europ?nne. European Conformity. |
| CFM | Cubic Foot per Minute |
| CFR | Code of Federal Regulations |
| CH | CHannel |
| CLK | CLocK. Acronym often used in signal name. |
| CLK1 | AdvancedTCA bused resource Synch clock group 1 |
| CLK2 | AdvancedTCA bused resource Synch clock group 2 |
| CLK3 | AdvancedTCA bused resource Synch clock group 3 |
| CMCI | Correctable Machine Check Interrupt |
| CMOS | Complementary Metal Oxide Semiconductor. Also refers to the small amount of battery (or capacitor) powered CMOS memory to hold the date, time, and system setup parameters. |
| COM | Serial port interface |
| COM.0 | PICMG COM Express(R) Module Base Specification |
| CPU | Central Processing Unit. This sometimes refers to a whole blade, not just a processor component. |
| CPUID | CPU IDentification. Code that uniquely identify a processor type. |

| Acronyms | Descriptions |
|---|---|
| CSA | Canadian Standards Association |
| CSM | Compatibility Support Module (UEFI/Legacy BIOS) |
| CSM16 | (Same as CSM). Compatibility Support Module (UEFI/Legacy BIOS) |
| DC | Direct Current |
| DCA | Direct Cache Access |
| DCD | Data Carrier Detect |
| DCU | Data Cache Unit |
| DB9 | D-subminiature 9 pins. Typically a serial port connector. DE-9 (D-sub connectors with a E size). |
| DDR | DDR SDRAM or Double-Data-Rate |
| DDR3 | DDR SDRAM or Double-Data-Rate 3rd Generation |
| DHCP | Dynamic Host Configuration Protocol |
| DIMM | Dual In-line Memory Module |
| DMA | Direct Memory Access |
| DMI | Desktop Management Interface |
| DRAM | Dynamic Random Access Memory |
| DTR | Data Terminal Ready |
| DTS | Digital Thermal Sensor in IA32 processors. |
| DVD | Digital Video Disk |
| ECC | Error Checking and Correction |
| EEPROM | Electrically Erasable Programmable Read-Only Memory |
| EFI | Extensible Firmware Interface |
| EHCI | Enhanced Host Controller Interface. Specification for Universal Serial Bus specification, revision 2.0. |
| EIA | Electronic Industries Alliance |
| EISA | Extended Industry Standard Architecture. Superset of ISA, 32-bit bus architecture. |
| EIST | (Same as SpeedStep). Enhanced Intel SpeedStep Technology |
| EMC | ElectroMagnetic Compatibility |
| EMI | ElectroMagnetic Interference |
| EMS | Emergency Management Services |
| EN | comit?Europ?n de Normalisation. European Committee for Standardization (English). The standards published by the European Committee for Standardization are recognizable by their prefix EN. |
| ESCD | Extended System Configuration Data |
| ESD | ElectroStatic Discharge |
| eUSB | Embedded Universal Serial Bus |
| FCC | Federal Communications Commission |
| FI | Fabric Interface. Backplane connectivity defined by the ATCA. |
| FIFO | First In First Out |
| FPGA | Field-Programmable Gate Array |
| FRU | Field Replaceable Unit. Any entity that can be replaced by a user in the field. Not all FRUs are hot swappable. |
| FTP | File Transfer Protocol |
| FW | FirmWare |
| GbE | Gigabit Ethernet |

| Acronyms | Descriptions |
|---|---|
| GND | GrouND |
| GT | Giga Transfer |
| GUID | Globally Unique Identifier |
| HDD | Hard Disc Drive |
| HECI | (Same as MEI) Host Embedded Controller Interface. The HECI bus allows the Host OS to communicate directly with the Manageability Engine (ME) integrated in the chipset. |
| HPM | PICMG Hardware Platform Management specification family |
| HPM.1 | Hardware Platform Management IPM Controller Firmware Upgrade Specification |
| HT | Hyper-Threading |
| HW | HardWare |
| I2C | Inter Integrated Circuit bus |
| IA-32 | (Same as IA32). Intel Architecture 32 bits |
| IA32 | (Same as IA-32). Intel Architecture 32 bits |
| ICH | I/O Controller Hub |
| ID | IDentification |
| IDE | Integrated Drive Electronics |
| IEC | International Electrotechnical Commission |
| IIO | Integrated I/O. Intel CPU with integrated Memory and PCIe. |
| IO | (Same as I/O). Input Output |
| IOH | I/O Hub |
| IOL | IPMI-Over-LAN |
| IP | Internet Protocol |
| IPM | Intelligent Platform Management |
| IPMB | Intelligent Platform Management Bus |
| IPMB-0 | Intelligent Platform Management Bus Channel 0, the logical aggregation of IPMB-A and IPMB-B. |
| IPMB-A | Intelligent Platform Management Bus A |
| IPMB-B | Intelligent Platform Management Bus B |
| IPMB-L | Intelligent Platform Management Bus Local |
| IPMC | Intelligent Platform Management Controller |
| IPMI | Intelligent Platform Management Interface |
| IRQ | Interrupt ReQuest |
| ISA | Industry Standard Architecture. 16-bit (XT) bus architecture. |
| KB | KiloByte |
| KCS | Keyboard Controller Style. An IPMI system interface. |
| LAN | Local Area Network |
| LED | Light-Emitting Diode |
| LPC | Low Pin Count port |
| LV | Low Voltage |
| MAC | Media Access Controller address of a computer networking device. |
| MCERR | Machine Check ERRor |
| ME | Management Engine |
| MEI | (Same as HECI) Management Engine Interface |

| Acronyms | Descriptions |
|---|---|
| MHz | MegaHertz |
| Microcode | Intel-supplied data block used to correct specific errata in the processor. |
| MMC | Module Management Controller. MMCs are linked to the IPMC. |
| MRC | Memory Reference Code. Chipset specific code provided by the manufacturer and integrated into the BIOS to test and intialize the system memory. |
| MTBF | Mean Time Between Failures |
| MTRR | Memory Type Range Register. CPU cache control registers. |
| NAND | Type of Flash Memory, used for mass storage. |
| NC | Not Connected |
| NCSI | (Same as NC-SI) Network Communications Services Interface |
| NC-SI | (Same as NC-SI) Network Communications Services Interface |
| NEBS | Network Equipment-Building System |
| NMI | Non-Maskable Interrupt |
| OEM | Original Equipment Manufacturer |
| OOS | Out Of Service |
| OS | Operating System |
| PCB | Printed Circuit Board |
| PCH | Platform Controller Hub. Southbridge from Intel. |
| PCI | Peripheral Component Interconnect |
| PCIe | (Same as PCI-E). PCI-Express. Next generation I/O standard |
| PCI-E | (Same as PCIe). PCI-Express. Next generation I/O standard. |
| PCI-X | PCI + minor changes to the protocol and faster data rate. |
| PDP | Project Development Process |
| PECI | Platform Environment Control Interface |
| PEF | Platform Event Filtering. An IPMI subfunction. |
| PET | Platform Event Trap. An IPMI message type. |
| PHY | PHYsical layer. Generic electronics term referring to a special electronic integrated circuit or functional block of a circuit that takes care of encoding and decoding between a pure digital domain (on-off) and a modulation in the analog domain. |
| PIC | Programmable Interrupt Controller |
| PICMG | PCI Industrial Computer Manufacturers Group |
| PICMG? | PCI Industrial Computer Manufacturers Group |
| PIR | Product Issue Report |
| PLD | Programmable Logic Device |
| PLL | Phase Lock Loop |
| POH | System Operating Power-On Hours. |
| POST | Power-On Self-Test |
| PPP | Point-to-Point Protocol |
| PROM | Programmable Read-Only Memory |
| PS | Primary Slave |
| PXE | Preboot eXecution Environment |
| QPI | QuickPath Interconnect. Point-to-point interconnect between Intel processors and IOH |
| RAID | Redundant Array of Independent Disks / Redundant Array of Inexpensive Disks. |

| Acronyms | Descriptions |
|---|---|
| RAM | Random Access Memory |
| RAS | Row Address Strobe, used in DRAM. May also refers to Reliability, Availability, Serviceability features of the chipset. |
| RDIMM | Registered Dual In-line Memory Module |
| RJ-45 | (Same as RJ45). 8P8C (8 Position 8 Contact) modular connector. |
| RJ45 | (Same as RJ-45). 8P8C (8 Position 8 Contact) modular connector. |
| RMCP | Remote Management Control Protocol |
| ROM | Read Only Memory. Also refers to option ROM or expansion ROM code used during POST to provide services for specific controllers, such as boot capabilities. |
| RS-232 | (Same as RS232). Recommended Standard 232. |
| RS232 | (Same as RS-232). Recommended Standard 232. |
| RTC | Real Time Clock |
| RTM | Rear Transition Module |
| RTS | Request To Send |
| S5 | ACPI OS System State 5. Indicates Soft Off operating state. |
| SAS | Serial Attached SCSI (Small Computer System Interface) |
| SATA | Serial ATA |
| SB | South Bridge |
| SCI | System Control Interrupt |
| SCL | Serial CLock |
| SCSI | Small Computer System Interface |
| SCU | Storage Control Unit |
| SDR | Sensor Data Record |
| SDRAM | Synchronous Dynamic Random Access Memory |
| SEL | System Event Log |
| SFP | Small Form-factor Pluggable |
| SFP+ | Small Form-factor Pluggable that supports data rates up to 10.0 Gbit/s. |
| ShMC | Shelf Management Controller |
| SIMD | Single Instruction, Multiple Data |
| SKU | Stock-Keeping Unit. Unique identifier for each distinct product and service that can be purchased. |
| SLP_S4 | S4 Suspend to Disk |
| SSC | Spread Spectrum Clock |
| SSD | Solid-State Drive |
| SMB | (Same as SMBus/SMBUS). System Management Bus. |
| SMBUS | (Same as SMB/SMBus). System Management Bus. |
| SMBus | (Same as SMB/SMBUS). System Management Bus. |
| SMI | System Management Interrupt |
| SOL | Serial Over LAN |
| SPD | Serial Presence Detect. A standardized way to automatically access information about a computer memory module. |
| SPI | Serial Peripheral Interface |
| SpeedStep | (Same as EIST). Enhanced Intel SpeedStep Technology. |
| SQTP | Software Qualification Test Plan |

| Acronyms | Descriptions |
|---|---|
| SWS | SoftWare Specification |
| TAP | Telocator Access Protocol. An IPMI Serial/Modem interface component. |
| TAP | Test Access Port |
| TBD | To Be Discussed or To Be Determined |
| TCC | Thermal Control Circuit |
| TCG | Trusted Computing Group |
| TCP | Transmission Control Protocol |
| TDC | Thermal Design Current |
| TDP | Thermal Design Power |
| TLP | Transaction Layer Packet |
| TPM | Trusted Platform Module |
| UART | Universal Asynchronous Receiver Transmitter |
| UDP | User Datagram Protocol. An Internet Protocol. |
| UEFI | Unified Extensible Firmware Interface |
| UL | Underwriters Laboratories inc |
| USB | Universal Serial Bus |
| VCC | Power supply |
| VCORE | Processor CORE power supply |
| VGA | Video Graphics Array |
| VLAN | Virtual Local Area Network |
| VLP | Very Low Profile |
| VMM | Virtual Machine Manager. Sometimes the third M is expanded to Monitor. |
| VT | Video Terminal |
| VTT | Power supply |
| VT100 | Video Terminal 100, this is a communication standard. |
| VT-d | Intel (R) Virtualization Technology for Directed I/O |
| VT-x | Intel (R) Virtualization Technology for IA-32 Intel (R) Architecture |
| WHEA | Windows Hardware Error Architecture |
| XAUI | X (meaning ten) Attachement Unit Interface. A standard for connecting 10 Gigabit Ethernet (10GbE) ports. |
| VCC | Power supply |
| VCORE | Processor CORE power supply |
| VGA | Video Graphics Array |
| VLAN | Virtual Local Area Network |
| VLP | Very Low Profile |
| VMM | Virtual Machine Manager. Sometimes the third M is expanded to Monitor. |
| VT | Video Terminal |
| VTT | Power supply |
| VT100 | Video Terminal 100, this is a communication standard. |
| VT-d | Intel (R) Virtualization Technology for Directed I/O |
| VT-x | Intel (R) Virtualization Technology for IA-32 Intel (R) Architecture |
| WHEA | Windows Hardware Error Architecture |
| XAUI | X (meaning ten) Attachement Unit Interface. A standard for connecting 10 Gigabit Ethernet (10GbE) ports. |